Metasploit 中文手册

wizardforcel

Published with GitBook

目錄

Metasploit v4 POC 上手指南

版本 1.0

亚太区总代理

企业版垂询：0755-33361000-846

企业版 KEY 申请：admin@metasploit.com.cn

目录

1. 介绍

Metasploit® 软件帮助安全专家和 IT 专家识别安全问题、验证漏洞修复情况，并管理由 专家执行的安全评估。 该产品提供真正的安全风险智能，帮助用户保护数据抵御攻击。

本 POC 指南的内容涉及智能入侵测定、密码审计、web 应用程序扫描和社会工程。Metasploit 帮助团队进行协作，并在整合的报告中显示其发现结果。

可以将利用 Metasploit Pro 进行的渗透测试分解成以下这些常规任务：

1. 创建项目

2. 发现设备

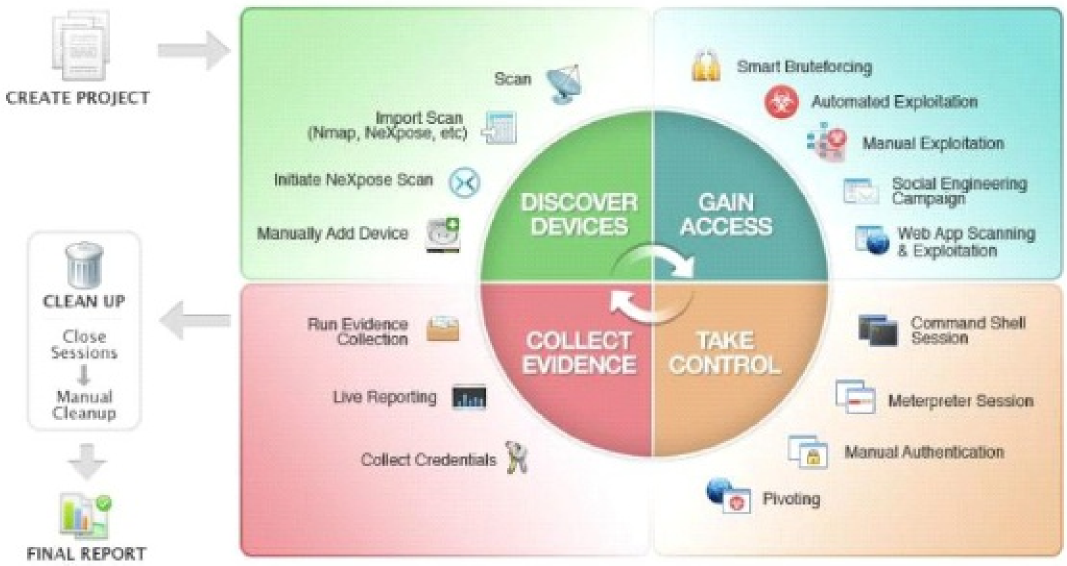
3. 获取对主机的访问权限

4. 控制会话

5. 从目标主机收集证据

6. 清除会话

7. 生成报告



2. 安装和初始化设置

本指南将在 Ubuntu Linux 10.04 x64 操作系统上安装 Metasploit Professional 版 本。 此外，将构建一个测试实验室来运行 POC。

2.1 前往 http://www.rapid7.com/products/metasploit/system-requirements.jsp 并检 查更新过的系统要求。

硬件要求

- 2 GHz+ 处理器
- 2 GB 内存（推荐 4 GB，根据相同设备上的虚拟机目标可能需要更高配置）
- 500MB+ 可用磁盘空间
- 10/100 Mbps 网卡

操作系统

- Windows XP、2003、Vista、2008 Server 和 Windows 7
- Red Hat Enterprise Linux 5.x、6.x - x86 和 x86_64
- Ubuntu Linux 8.04、10.04 - x86 和 x86_64

浏览器版本

- Mozilla Firefox 4.0+
- Microsoft Internet Explorer 9
- Google Chrome 10+

2.2 要下载 Metasploit 安装程序，请前往 http://metasploit.com/download/ 并下载正 确的安装程序。 可以在此处找到 Professional、Express、Framework 和 Community 版本。 应下载 Professional 版本来运行 POC。



2.3 要获取文档（例如安装指南和用户指南等），请访问

https://community.rapid7.com/community/solutions/metasploit?view=documents

2.4 （下方是针对 Ubuntu linux 的配置说明，如果需要安装在其他操作系统上，请参阅 安装指南。 安装程序文件名在您的 POC 中可能有所不同。） 打开命令提示框并前往 Metasploit 安装程序所位于的文件夹，使用 `sudo -i` 命令并输入密码来获得超级 用户特权。 使用 `chmod +x metasploit-latest-linux-x64-installer.run` 命令， 将执行文件属性添加到此安装程序。

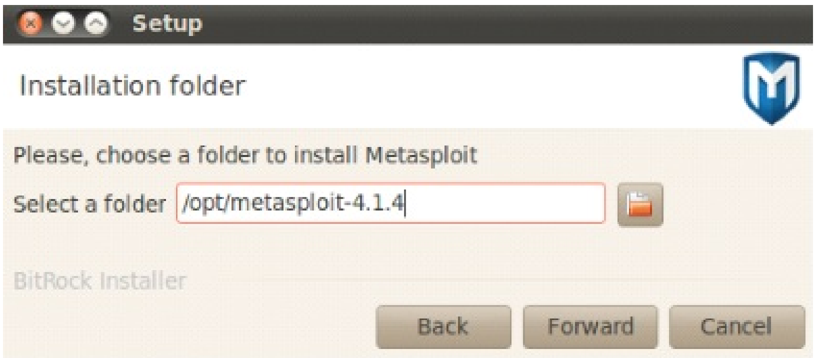
```
root@ubuntu:/home/mlai# chmod +x metasploit-latest-linux-x64-installer.run
root@ubuntu:/home/mlai# ls -al metasploit-latest-linux-x64-installer.run
-rwxrwxrwx 1 mlai mlai 245241294 2012-01-09 12:51 metasploit-latest-linux-x64-in
staller.run
root@ubuntu:/home/mlai# ./metasploit-latest-linux-x64-installer.run
```

2.5 使用 `./metasploit-latest-linux-x64-installer.run` 命令来运行此安装程序。 阅读并接受许可协议。 点击 `Forward` （下一步）继续。





2.6 选择安装文件夹。 如果安装了主机反病毒程序，应将此文件夹添加到 AV 白名单中。



2.7 决定是否要将 Metasploit 安装为自动启动的服务。 这一步将添加一个初始化脚本， 以便在启动时调用 $INSTALLERBASE/ctlscript.sh。



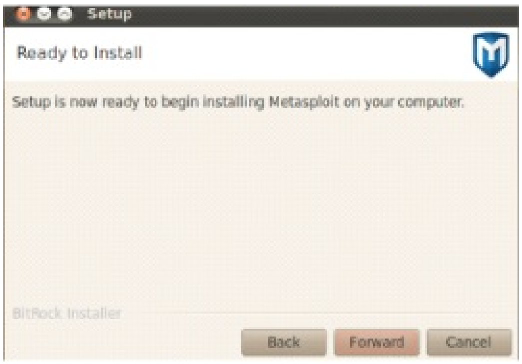
2.8 接下来两步是接受 3790 端口作为默认的 Web GUI 端口或输入其他端口，并为 Web GUI 的 HTTPS 连接生成 SSL 证书。





2.9 其后两步是启用/禁用自动更新并开始运行安装程序。



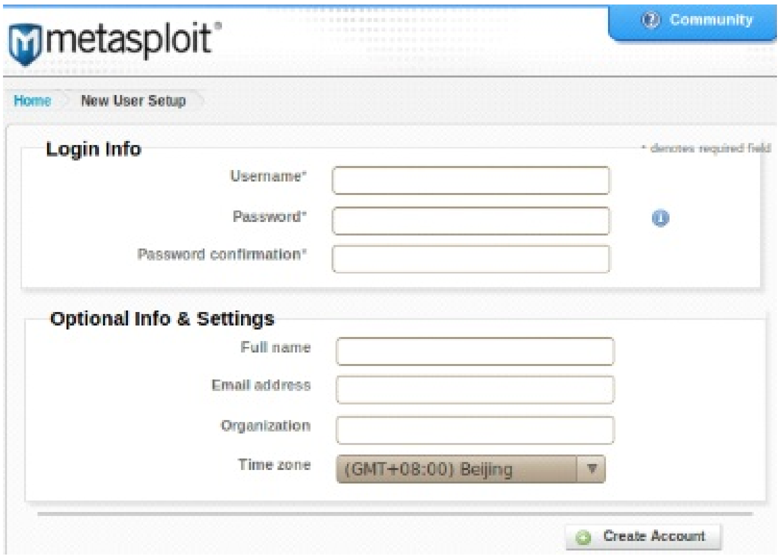


2.10 要管理 Metasploit 服务，请前往安装文件夹并使用以下命令：

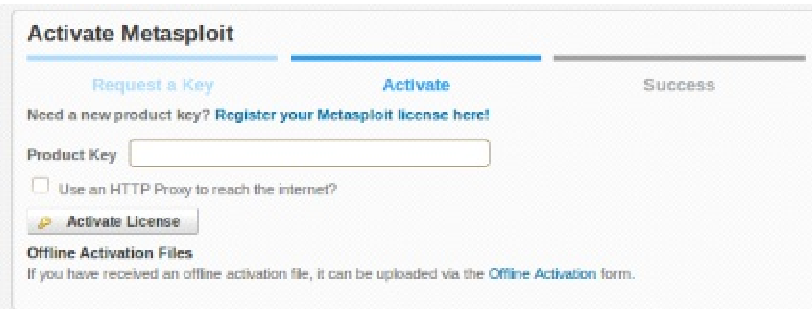
- 使用 `./ctlscript.shstart` 命令来启动服务
- 使用 `./ctlscript.sh status` 命令来检查服务状态
- 使用 `./ctlscript.sh stop` 命令来停止服务

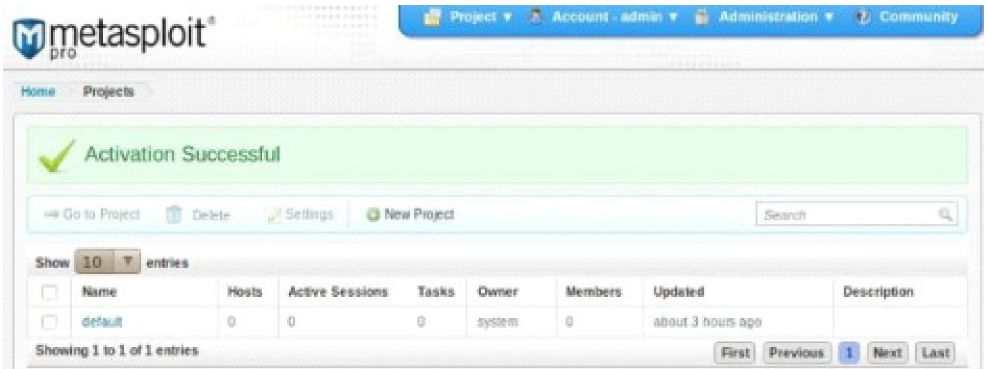
```
root@ubuntu:/opt/metasploit-4.1.4# pwd
/opt/metasploit-4.1.4
root@ubuntu:/opt/metasploit-4.1.4# ./ctlscript.sh start
LOG:  database system was shut down at 2012-01-09 15:47:08 HKT
LOG:  database system is ready to accept connections
LOG:  autovacuum launcher started
/opt/metasploit-4.1.4/postgresql/scripts/ctl.sh : postgresql  started at port 73
37
prosvc is running
metasploit is running
root@ubuntu:/opt/metasploit-4.1.4#
```

2.11 要运行初始化设置，请打开本地浏览器并访问 https://127.0.0.1:3790。 在初始 化完成前不允许连接远程浏览器。 输入登录信息。



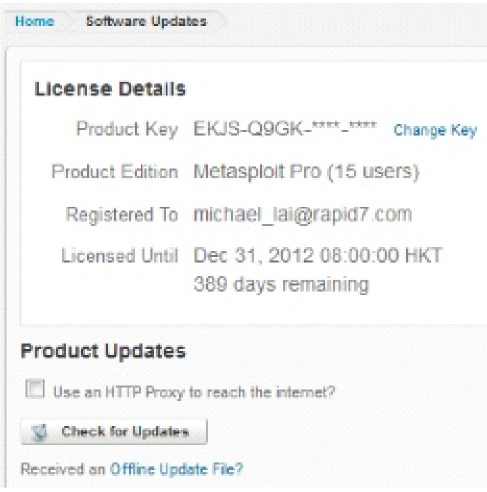
2.12 在另一个屏幕上，输入激活许可证。 请确保可以访问 `updates.metasploits.com`， 因为该站点或 IP 可能被归入 `黑客` 类别而受到 web 过滤解决方案的阻止。 如果您没有密钥，您可以点击 `Register your Metasploit license here!` （在此处注册您的 Metasploit 许可证！）来获取密 钥。





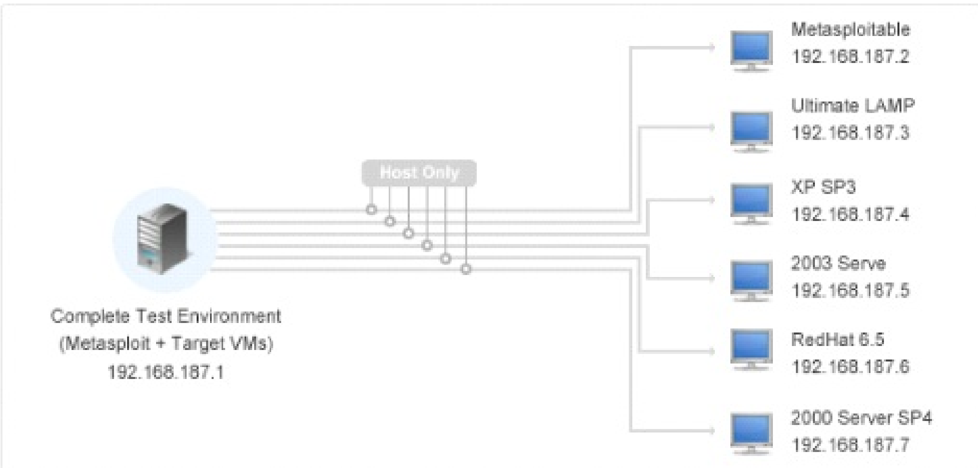
2.13 前往 Administration > Software Updates （管理 > 软件更新），并确保所有 信息（产品密钥、产品版本、注册到、许可证过期日期）都准确无误。 点击 Check for Updates （检查更新）。 必要时请设置 HTTP 代理服务器。





2.14 要构建测试实验室，请前往 http://www.metasploit.com/help/test-lab.jsp，您 将找到 Metasploit 的测试实验室网络结构。 这些系统可以是虚拟机镜像或在工作站/服务器硬件上运行的实际操作系统。

- Metasploit 控制台： 安装托管 Metasploit 的操作系统。
- Metasploitable： 具有大量漏洞的 Linux 主机
- Ultimate LAMP： 具有大量漏洞的 web 应用程序服务器
- XP SP3： 其他 XP 服务包级别或 Windows 7 尤佳
- 2003 Server： 具有服务包级别的 2008 Server 尤佳



2.15 要下载 Metasploitable，请在上述网页上搜索 `download the Metasploitable machine using BitTorent` （使用 BitTorent 下载 Metasploitable 机器）。 下载 种子，然后下载 Metasploitable 虚拟机镜像。 在 VM Workstation 或 VM Player* 中运行该文件。登录 ID 和密码分别是 `msfadmin` 和 `msfadmin` 。

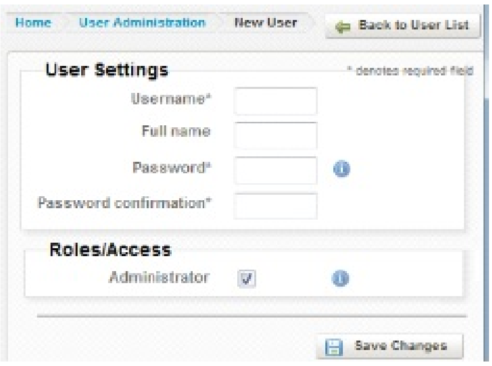
*VM Player 是免费软件，但是只允许一个镜像。 VMWare 网站上提供 VM Workstation 试用版。

2.16 要下载 Ultimate LAMP：请在上述网页上搜索 `You can download UltimateLAMP here` （您可以从此处下载 UltimateLAMP）。 下载 Ultimate LAMP VM 镜像。 在 VM Workstation 或 VM Player 上运行该文件。 登录 ID 和密码分别是 `vmware` 和 `vmware` 。

2.17 至于 Windows 域环境，您需要自行准备一台 Windows 服务器和一台 Windows 工 作站。

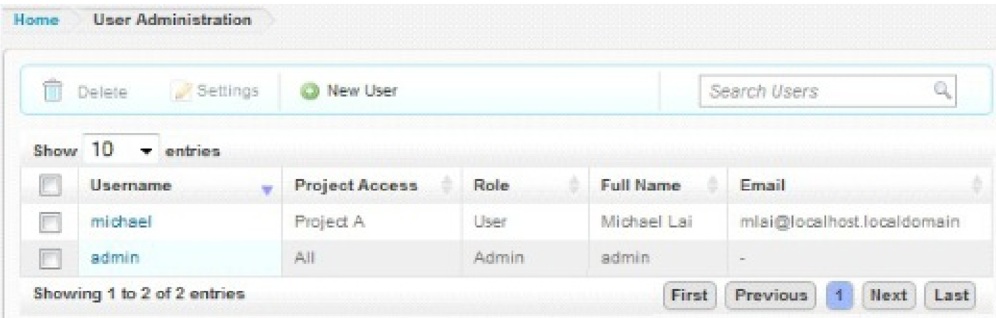
3. 用户和项目

项目提供一种方式来组织并整理您的渗透测试。 使用名称、网络边界和授权用户来创建 项目。 网络边界帮助您设置和保持一个范围。 可以在项目中添加或删除个人。 获得项 目访问权限的任何人都具有完整的特权。

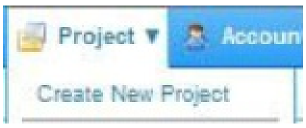


3.1 要进行用户管理（添加、删除和设置密码），请前往 `Administration > User Administration` （管理 > 用户管理）并点击 `New User` （新建用户）来添加新用 户。 `Administrator` （管理员）角色可以访问所有项目、管理用户并应用软件更 新。 （该许可证必须支持多个用户，以便添加新用户）。

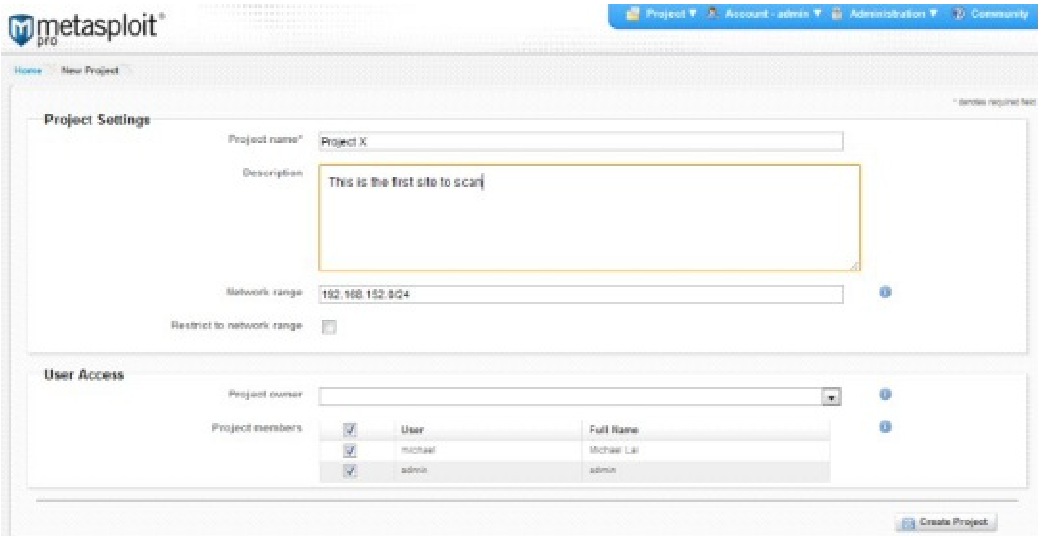


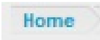
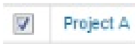


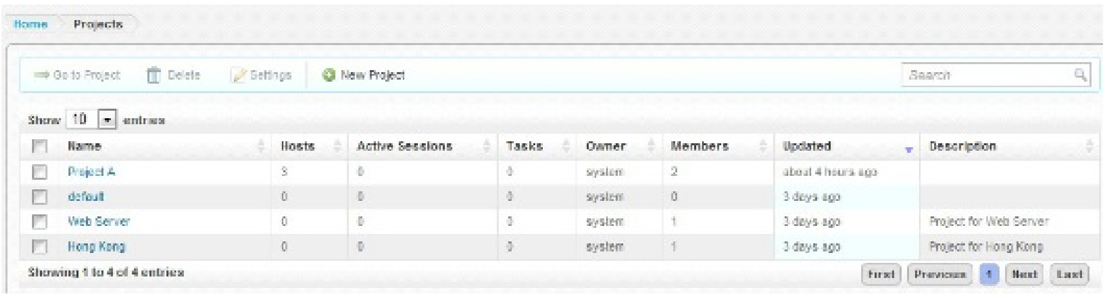
3.2 要新建项目，请前往 `Project > Create New Project` （项目 > 新建项目）。



3.3 输入项目名称、描述、网络范围、项目拥有者和成员。 网络范围也就是该项目的界 限。



3.4 点击  Home （主页） 即可显示所有可用项目。 要编辑项目，勾选  并点击 Settings （设置）  。

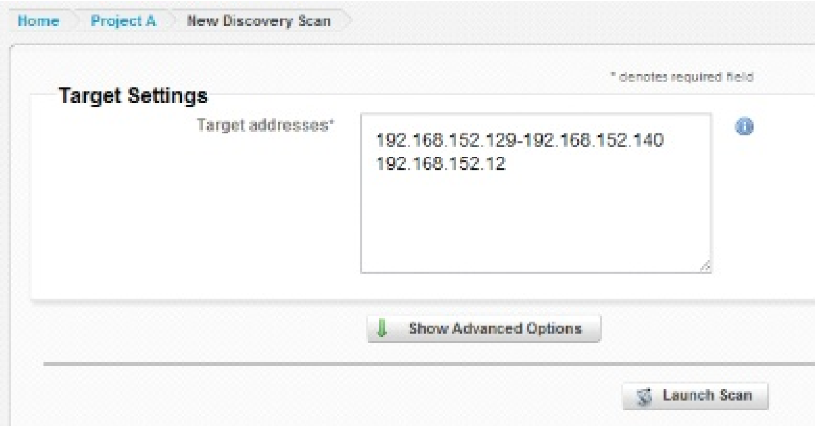


4. 发现设备

运行渗透测试的第一步是发现一些目标。 Metasploit 可以使用内置的工具和模块来进行 扫描并发现设备，从其他工具导入结果，对目标网络使用 Nexpose 来发现漏洞。

4.1 前往该项目并点击 

按钮。 输入要执行发现操作的地址（范围）。



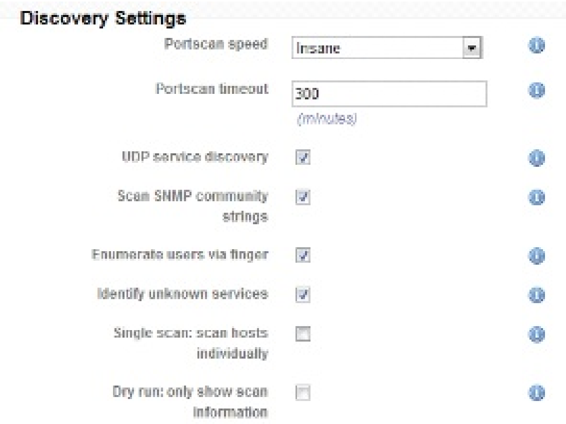
4.2 点击 

来自定义扫描。 可以找到 Nmap 参数和端口设置。 将鼠 标移至  来获得帮助。 在 `Advanced Target Settings` （高级目标设置）下方，

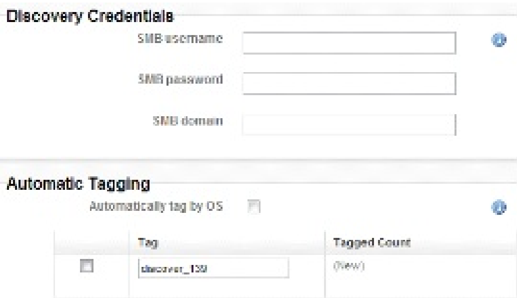
您可以自定义 NMAP 参数、源端口和目标端口。



4.3 在 `Discovery Settings` （发现设置）下方，可以设置扫描速度和超时来控制网络 使用。在此处启用的选项越多，扫描就越慢。 如果选择 `Dry run` （预检）， Metasploit 不会扫描网络，但是任务日志将显示相关信息。



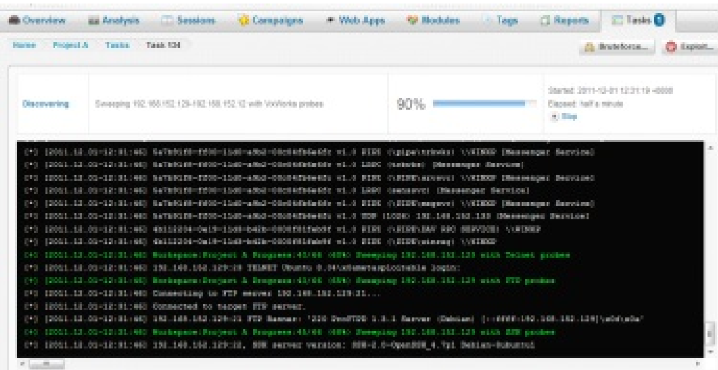
4.4 在 `Discovery Credentials` （发现凭证）下方，可以设置 SMB 凭证来进行共享并 发现 Windows 网络中的用户名。 在 `Automatic Tagging` （自动添加标签）下方， 可以自动添加操作系统标签，这样您便能基于操作系统（例如 Linux）更简便地管理 主机了。



4.5 点击右下角的 `Launch Scan` （启动扫描）。 

一旦开始扫描，就会在 `Tasks` （任务）选项卡 

上显示 `Discovering` （发现）任务。

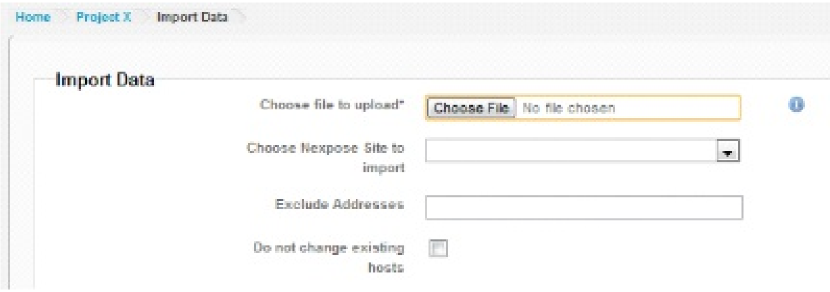


4.6 除了 Metasploit 发现的设备以外，还可以导入设备列表。 点击项目主页上的 

。 将鼠标移至  来查看支持的所有文件类型。

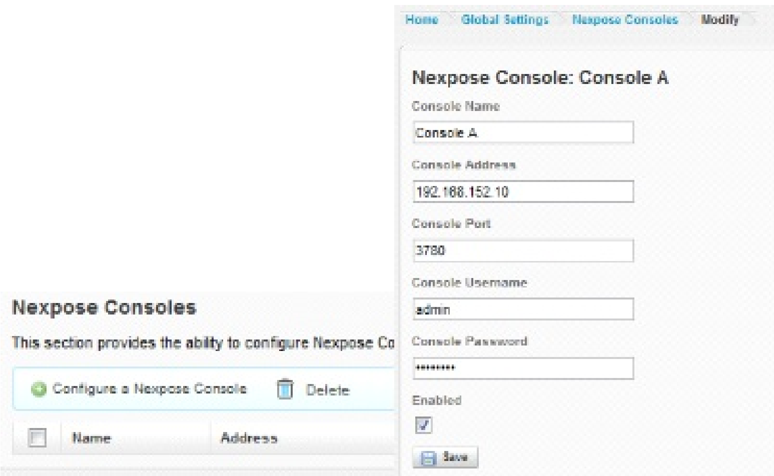


4.7 选择要排除的文件、站点和地址。 点击 Import Data 。

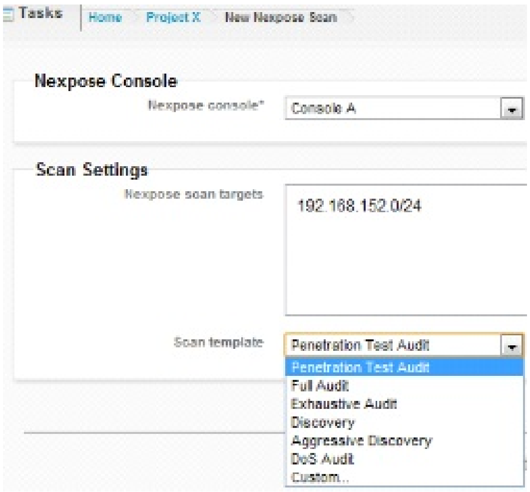


4.8 Metasploit 可以启动 Nexpose 来执行设备发现操作。 前往 `Administration` （管 理）选项卡并点击 `Global Settings` （全局设置）。 向下滚动鼠标至 `Nexpose Consoles` （Nexpose 控制台）部分并点击 Configure a Nexpose Console 。 输入信息来 添加 Nexpose 控制台。

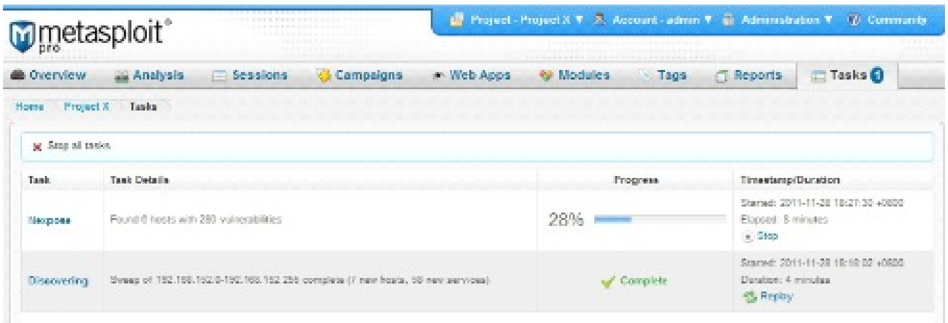




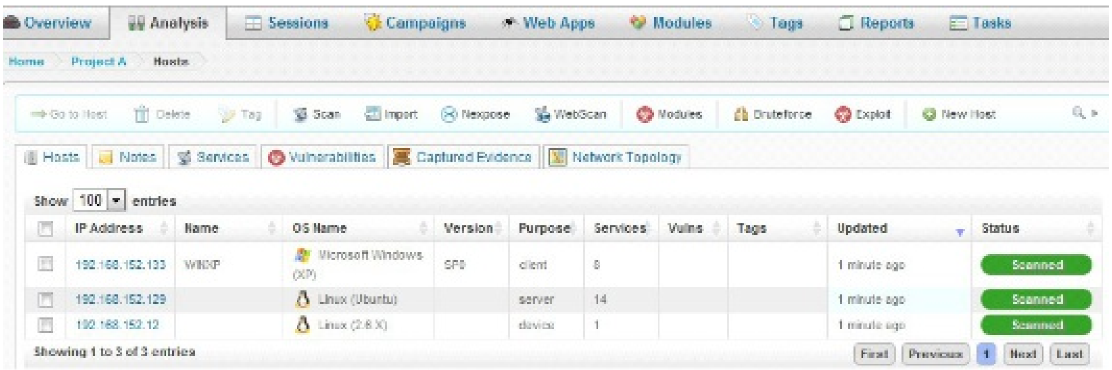
4.9 要启动 Nexpose 扫描，在项目主页上点击 Nexpose。 选择新添加的 Nexpose 控制 台，指定 IP/IP 范围和 `Scan template` （扫描模板）。 点击右下角的 Launch Nexpose 来启动扫描。



4.10 一旦启动 Nexpose 进行扫描，就会在 `Tasks` （任务）选项卡上显示相关信息。



4.11 完成扫描后，主机选项卡 `Analysis > Hosts` （分析 > 主机）将显示检测出易 受入侵的主机。



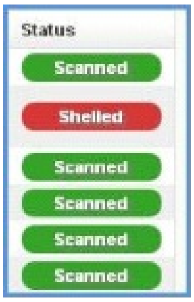
4.12 最后一栏是主机状态。 这些状态如下所示：

1. Scanned（已扫描）– 已发现设备。

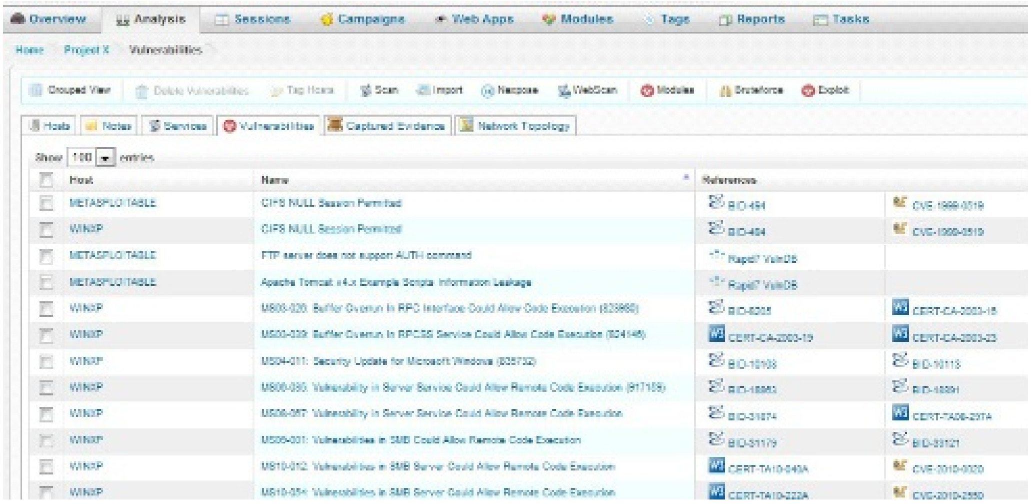
2. Cracked（已破解）– 已成功地强力破解凭证，但尚未获取会话。

3. Shelled（已攻陷）– 已获取设备上打开的会话。

4. Looted（已掠取）– 已从设备收集证据。



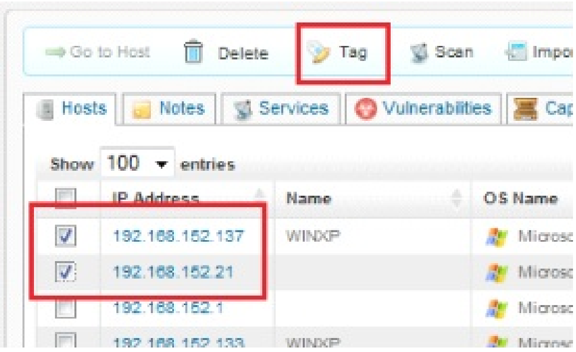
4.13 如果启动 Nexpose 来发现设备，您可以查看易于受到入侵的漏洞列表。 前往 `Analysis > Vulnerabilities` （分析 > 漏洞）。 将显示找到的所有主机的漏 洞。 点击 `reference` （参考）图标来检查来自网络的漏洞信息，这样便能选择特 定的模块来入侵主机了。

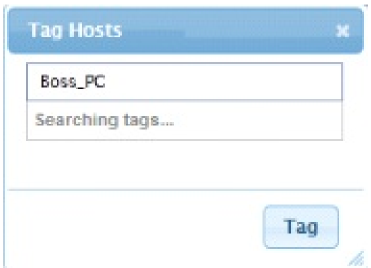


4.14 标签有助于对主机进行分组。 例如：您可以利用相同的标签（例如 `os_windows` ）为所有主机生成一份报告。 如果已启用 4.4 中提到的 `Automatic Tagging` （自动添加标签）功能，主机表格将显示检测出的操作系统标签。

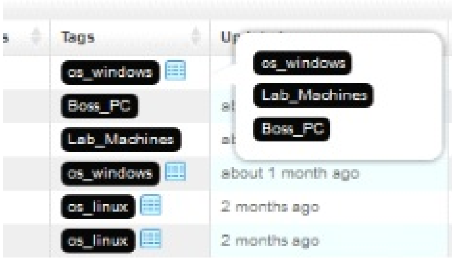


4.15 要添加您的标签，请选择主机然后点击 Tag 。 输入标签名称然后点击 Tag 。

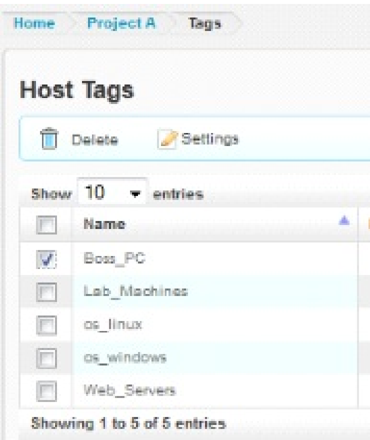




4.16 某些主机可能拥有多个标签。 将鼠标移至 Tags （标签）栏下方的。 将显 示所有标签。

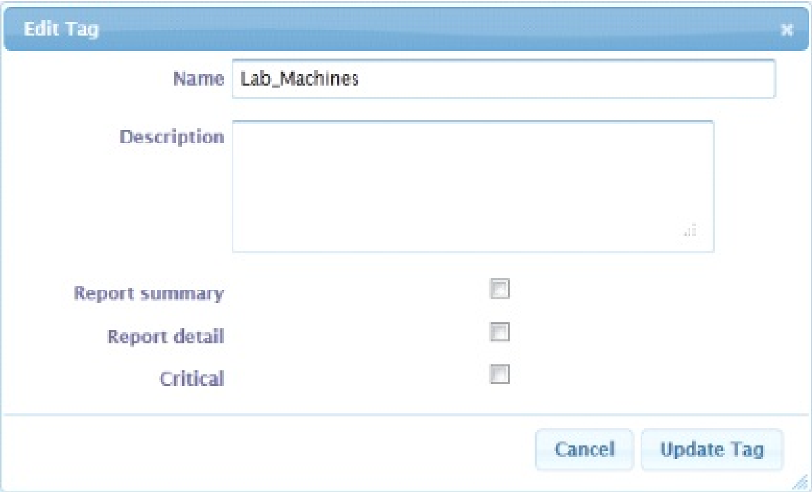


4.17 点击 Tags 以便进入 Tags （标签） 页面。 要删除标签，请将其选定并点击 Delete 。 您可以同时选择和删除多个标签。





4.18 要管理标签，请选择一个标签并点击 Settings 。您可以更改名称、添加描述并设置 `Report summary` （报告摘要）、 `Report detail` （报告详细信息）和 `Critical` （关键）。这三个标签表示以报告摘要、报告详细信息和关键的发现 结果来描述主机。



下方是标签 `Lab_Machines` 的 `Report summary` （报告摘要）示例。

Major Findings

Tagged Hosts

Tag	Address	Hostname	Description
Lab_Machines	192.168.152.129	METASPLOITABLE	
Lab_Machines	192.168.152.133	WINXP	
Lab_Machines	192.168.152.12	192.168.152.12	
Lab_Machines	192.168.152.1	192.168.152.1	
Lab_Machines	192.168.152.137	WINXP	

5. 入侵基本原理

本章将说明管理入侵和强力攻击的基本组件。 这些组件包括有效载荷、客户端/服务器端 攻击和模块。

5.1 有效载荷： 提供两个针对入侵和强力攻击的有效载荷选项。 如果选择 Meterpreter 不起作用，则使用 Command Shell。

5.2 Meterpreter 是 Metasploit 有效载荷，为攻击者提供交互式的外壳（shell）。例 如：利用 VNC 控制设备的屏幕并浏览、上传和下载文件。 该选项能够完成大量入侵 后任务并进行定制，例如在网络内运行脚本自动化入侵。 将在以下情况创建 Meterpreter 会话：

- 成功入侵 Windows
- 对 Windows 进行 SSH 强力攻击
- 对 Windows 进行 Telnet 强力攻击
- 对 Windows 进行 SMB 强力攻击
- 对 Windows 进行 Tomcat 强力攻击

5.3 Command Shell 帮助用户对主机运行收集脚本或运行任意命令。 将在以下情况创建 Command Shell 会话：

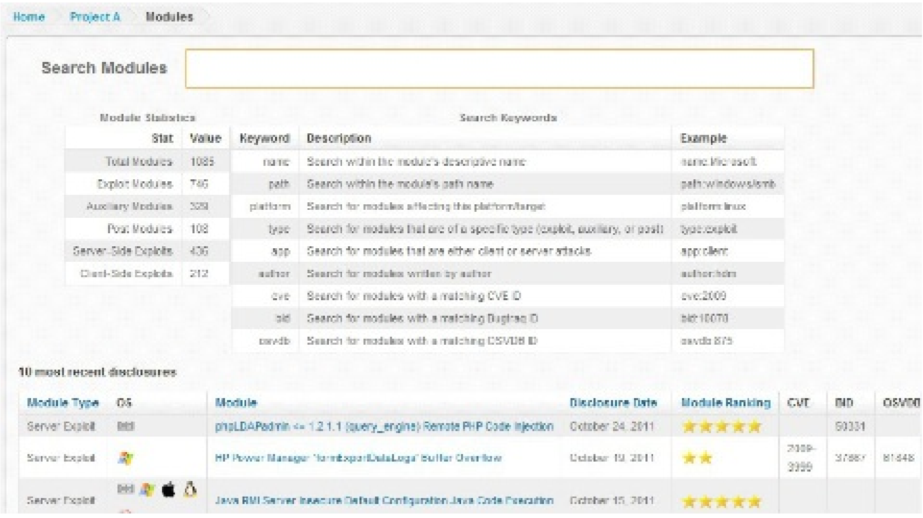
- 成功入侵 *nix
- 对 *nix 进行 SSH 强力攻击
- 对 *nix 进行 Telnet 强力攻击
- 对 *nix 进行 Tomcat 强力攻击

5.4 模块： 任何人都可以开发模块，为社区做出贡献。

- 充分利用一处的所有 Metasploit 模块
    - 通过关键字轻松简便地使用搜索界面
    - 可以扩展所有标准入侵来瞄准一定范围
    - 使用任何您已知的首选模块
- 细粒度控制模块选项
    - 指定并覆盖任何标准选项
    - 使用 Advanced（高级）和 Evasion（闪避）选项

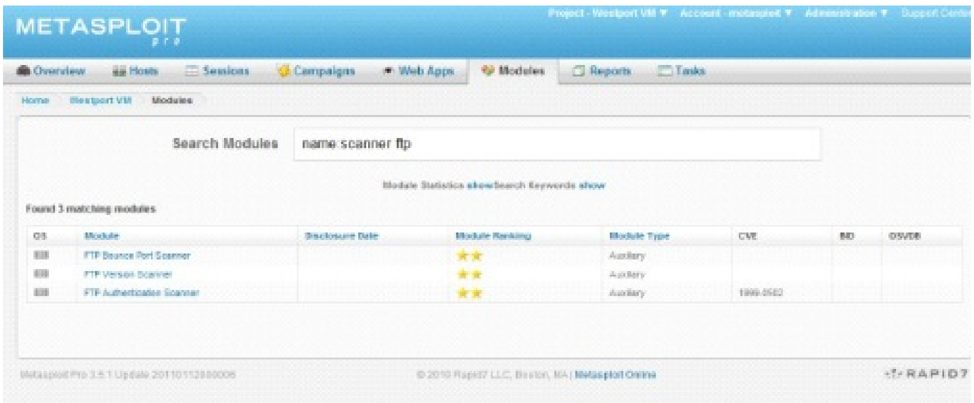
- 基本自动化有效载荷的选择
    - 选择 Meterpreter vs Shell
    - 选择 Reverse（反向）vs Bind（绑定）
    - 选择端口范围

5.5 Click the  在菜单栏上将显示模块统计和搜索关键字格式



.

5.6 要搜索模块，请输入 `name: vulnerability_keyword` 或 `cve-xxxx-xxxx` 。 例如： `name:scanner ftp` 。

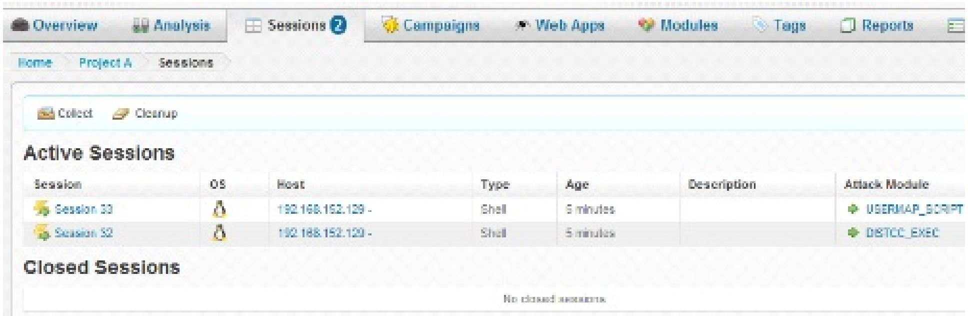


5.7 服务器端入侵： Metasploit 将作为客户端连接到服务器并进行入侵。 例如： Metasploit 连接到 HTTP 服务并入侵 web 应用程序。 要搜索用来入侵服务器的模 块，请搜索 `app:server` 。



5.8 客户端入侵： 可以设置 Metasploit 监听服务并让客户端进行访问。 一旦建立了连 接，Metasploit 将尝试入侵客户端。 在本例中，Metasploit 将作为服务器并入侵客 户端。 要搜索用来入侵客户端的最新模块，请搜索 `app:client` 。

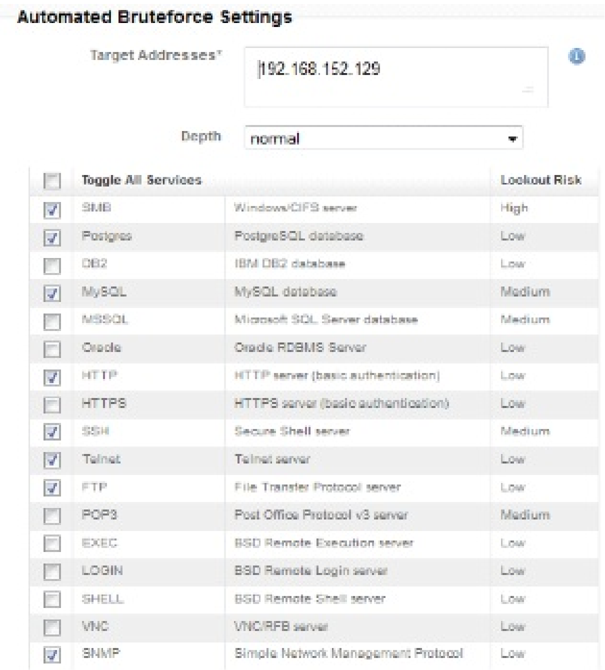
5.9 会话： 一旦 Metasploit 入侵了主机，就会构建一个会话。 会话是与主机建立的连 接，并让您在主机上 `执行某些操作` ， 例如复制文件。



6. 强力攻击

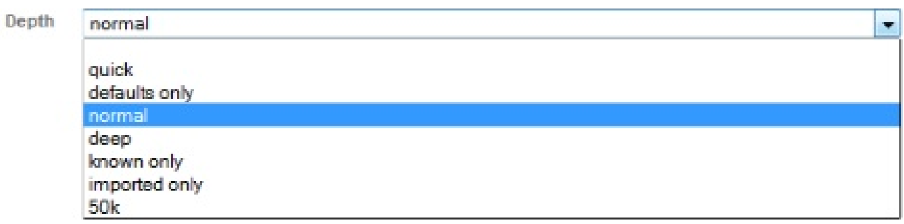
强力攻击这种技术通过尝试不同的凭证来获取访问权限。 一旦使用了正确的用户 ID 和 密码，Metasploit 就能自动登录。

6.1 选择一个项目或主机，然后点击 Bruteforce 来进入 `Bruteforce` （强力攻击）页面。 必要时请编辑目标地址并选择要对其进行强力攻击的服务。



6.2 `Depth` （深度）级别定义密码的位数和复杂性。

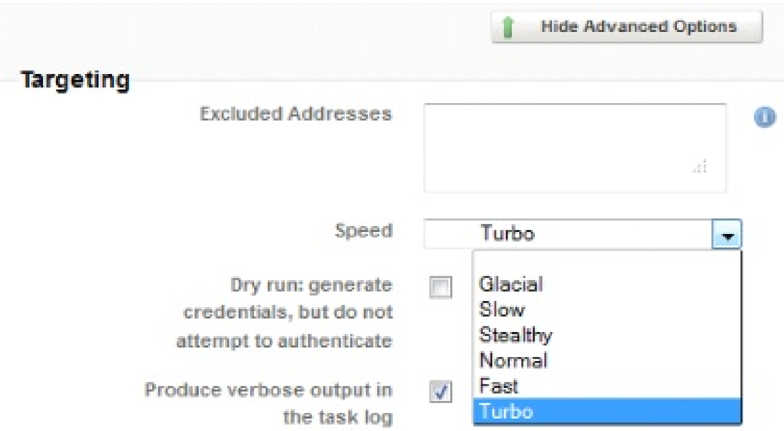
- Quick（快速）： 简单的默认用户名和密码，小型静态列表
- 默认： 由制造商/ISP 设置的常见密码，已知后门
- 常规： 从扫描数据自动生成凭证，极少视协议而定的用户名和大量常见密码
- 深入： 额外的常见密码词表，不适用于较慢的服务，例如 Telnet 和 SSH。



6.3 Show Advanced Options 按钮将允许您自定义 `Target` （目标）、 `Credential Selection` （凭证选择）、 `Playload` （有效载荷）、 `Bruteforce Limiter` （强力攻击限制器）、 `Credential Generation` （凭证生成）和 `Credential Mutation` （凭证变化）。

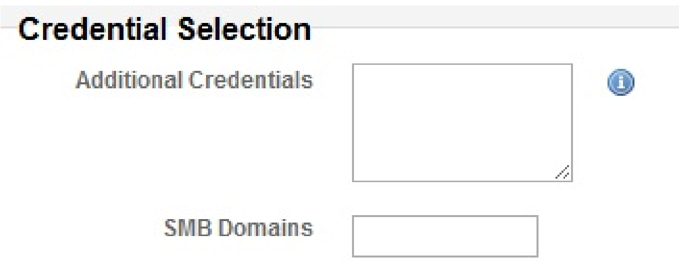
6.4 在 `Targeting` （目标）部分下方，您可以排除目标、设置速度、启用 `Dry run` （预检）和详细日志。

- 选择适用于您网络带宽的 `Speed` （速度）。
- `Dry run` （预检）仅生成凭证，但不会强力攻击目标主机。

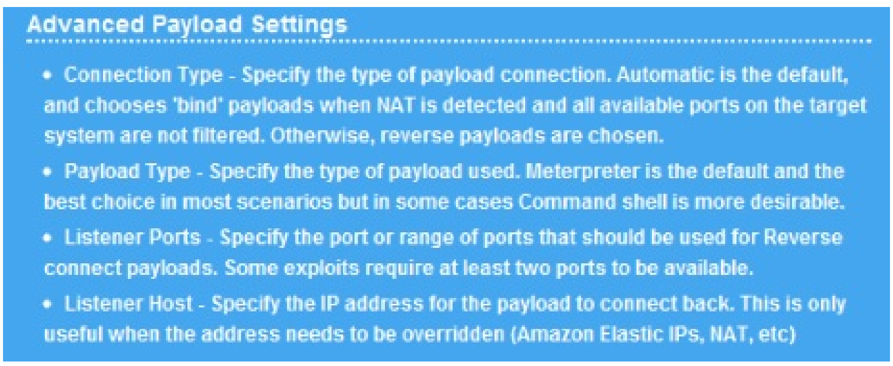


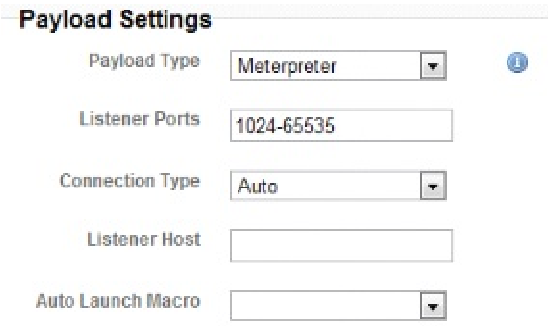
6.5 在 `Credential Selection` （凭证选择）部分下方，您可以使用以下格式（仅接受 密码或用户名）添加额外的凭证。 您还可以指定 SMB 域。

- domain/username pass1 pass2 pass3
- username pass1 pass2 pass3
- <blank> pass1 pass2 pass3
- username

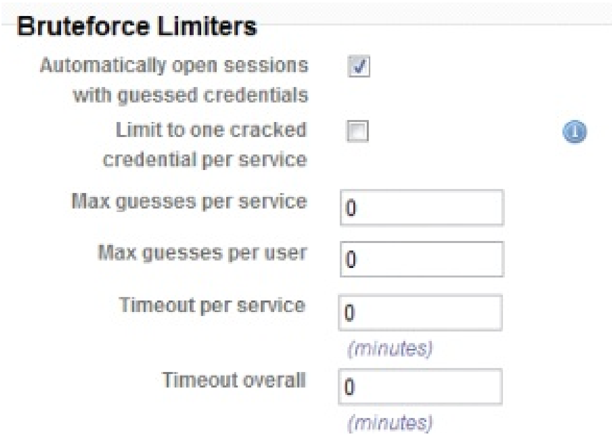


6.6 在 `Payload Settings` （有效载荷设置）下方，您可以自定义有效载荷。 通常使用 默认值。 请参阅 5.1 有效载荷获得更多信息。

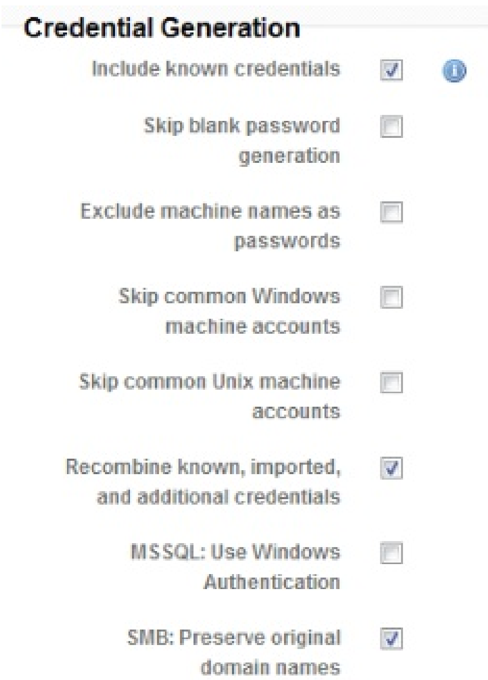


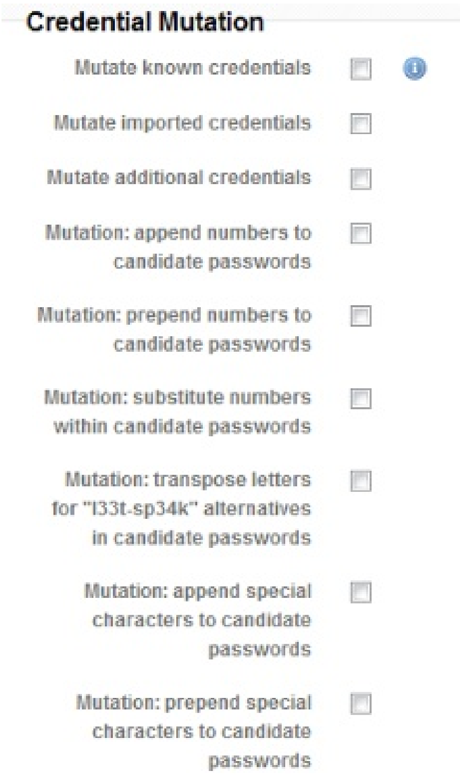


6.7 在 `Bruteforce Limiters` （强力攻击限制器）部分下，设置一些参数的限制，例如 每个用户、服务的密码猜测最多次数。 `Automatically open sessions with guessed credentials` （使用猜测的凭证自动打开会话）将利用成功的验证（例如 SSH）构建会话。

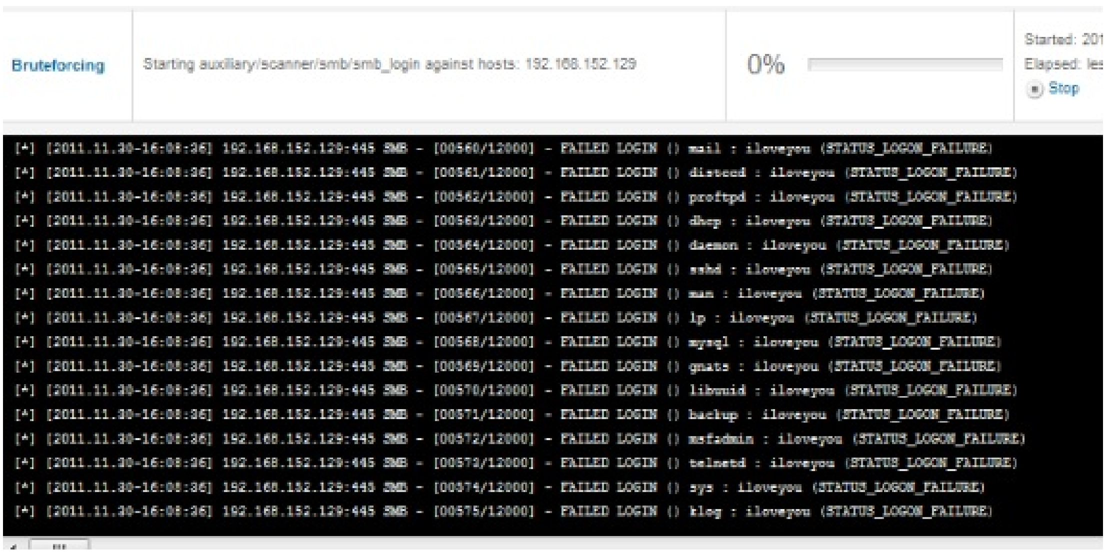


6.8 `Credential Generation` （凭证生成）和 `Credential Mutation` （凭证变化） 允许您微调 Metasploit 生成凭证的方式。

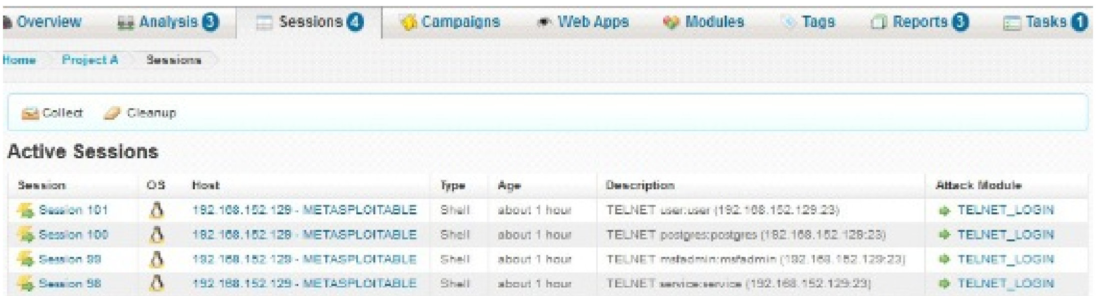




6.9 点击 Launch Bruteforce 来启动强力攻击任务。 该 GUI 显示处于强力攻击下的服务（例 如 SMB）、使用的凭证和结果。

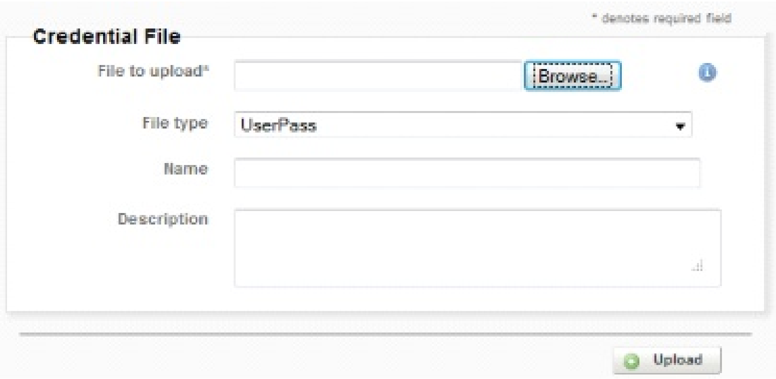


6.10 如果对目标进行了成功的强力攻击， `Sessions` （会话）选项卡将显示连接的会 话。



6.11 要使用您自己的词典，请点击 Bruteforce 进入 `Bruteforce` （强力攻击） 页面。

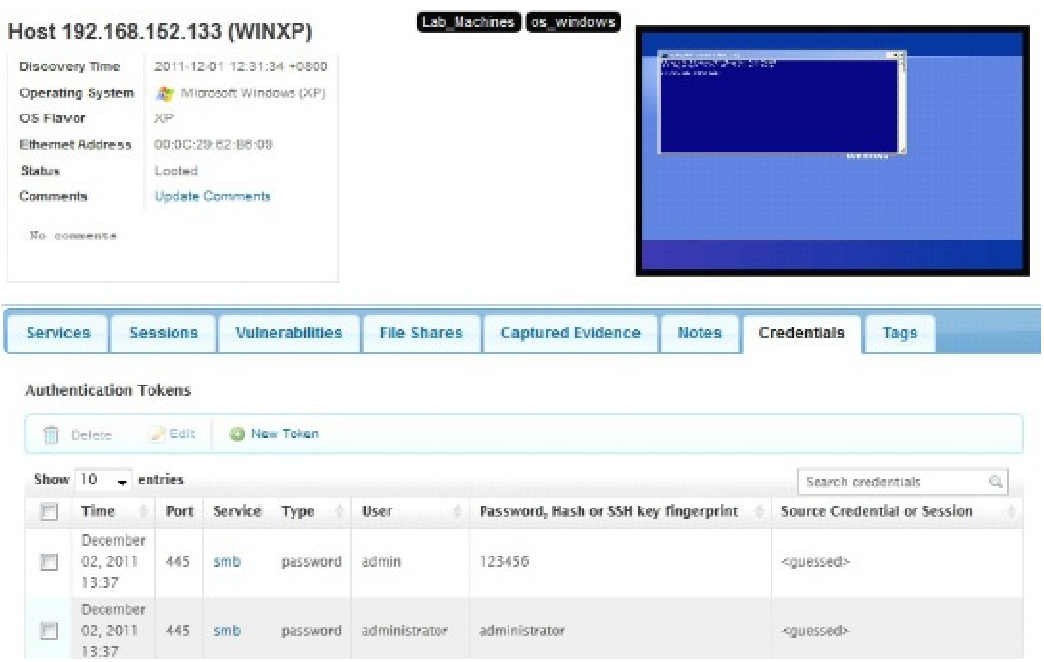
点击左上角的 Manage Credentials 。 您可以在新页面中上传您的凭证文件。 将鼠标 移至 来获取有关文件格式的更多信息。



6.12 在 `Bruteforce` （强力攻击） 页面上，为 `Depth` （深度） 选择 `imported only` （仅导入） 。 必要时在发动强力攻击之前进行其他高级配置。



6.13 要检查从强力攻击收集而来的凭证，请前往 `Analysis > Hosts` （分析 > 主 机）并从表格中选择主机。 `Credentials` （凭证）选项卡将显示强力攻击找到的 凭证，以及猜测情况。

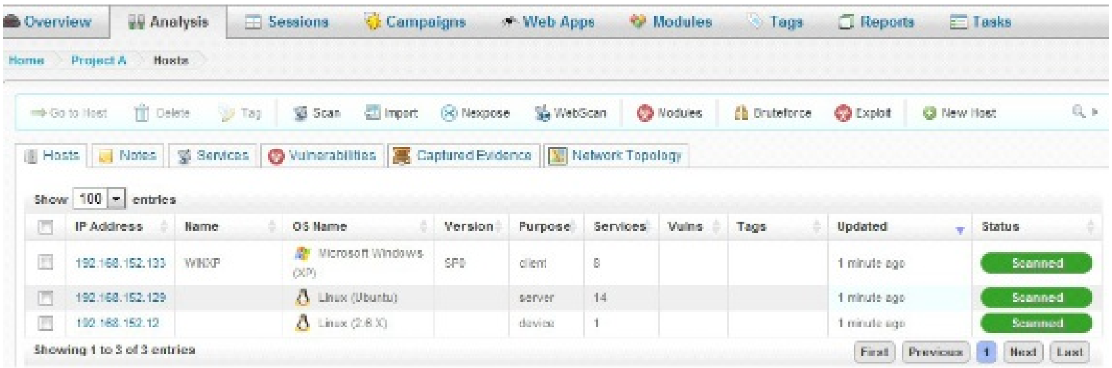


7. 入侵

本章将通过 Metasploit 利用服务入侵主机来说明服务器端入侵。

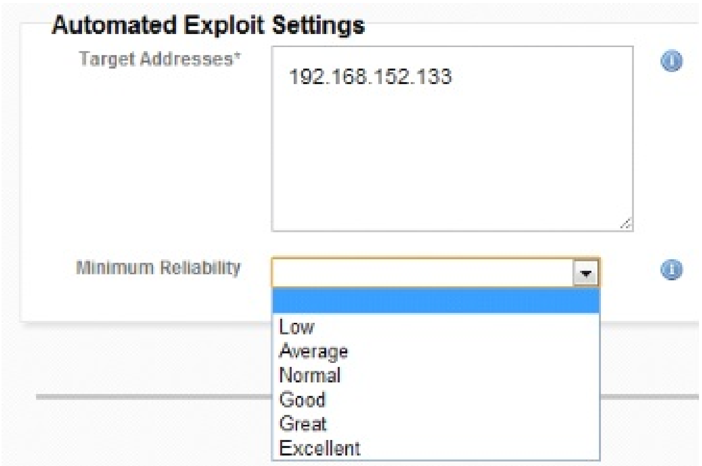
7.1 要入侵主机，请前往主机选项卡 `Analysis > Hosts` （分析 > 主机）。 选择主机 然后点击 

按钮。



7.2 在 `Automated Exploit Settings` （自动化入侵设置）部分下方，确认目标 IP 地 址是否正确。 选择 `Reliability` （可靠性）级别来实现成功入侵几率和损坏目标 几率之间的平衡。

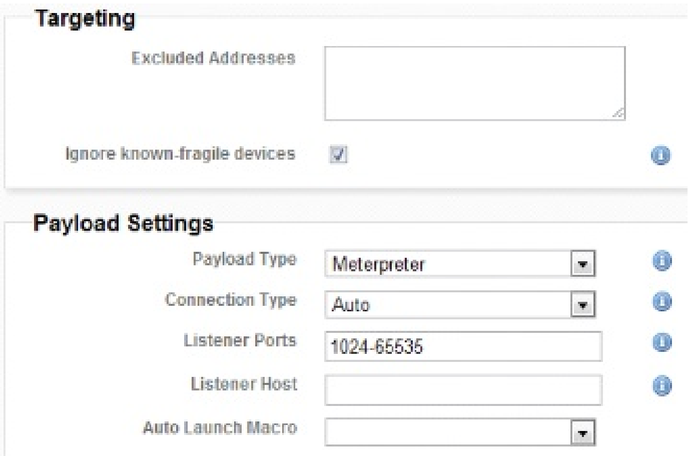
- Low（低） ： 损坏和入侵的几率最高
- Excellent（极好） ： 不会使目标崩溃，而且避免大量高风险的操作



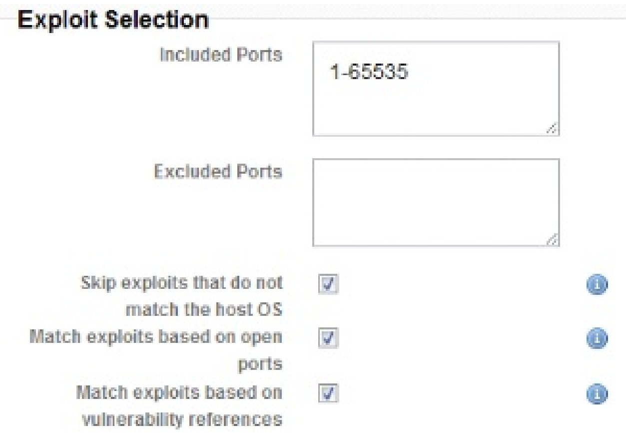
7.3 点击 

来访问高级选项，例如 `Targeting` （目标）、 `Payload Settings` （有效载荷设置）、 `Exploit Selection` （入侵选择）和 `Advanced Settings` （高级设置）。

7.4 `Targeting` （目标）部分允许您排除地址并忽略已知易受入侵的设备。 `Payload Settings` （有效载荷设置）与 `Bruceforce 6.6` （强力攻击 6.6）相同。



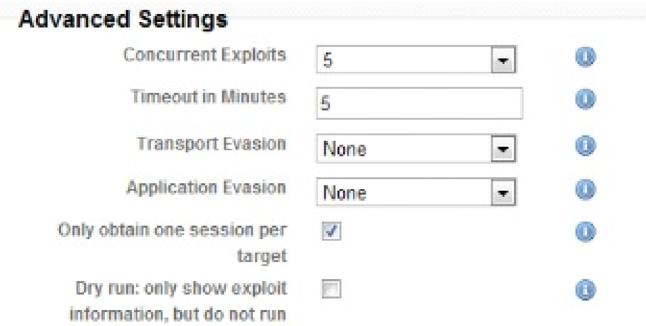
7.5 在 `Exploit Selection` （入侵选择）部分下，您可以为入侵设置端口并删除不太相 关的模块。 可以利用主机操作系统、开放的端口和漏洞参考来匹配将要使用的入侵。



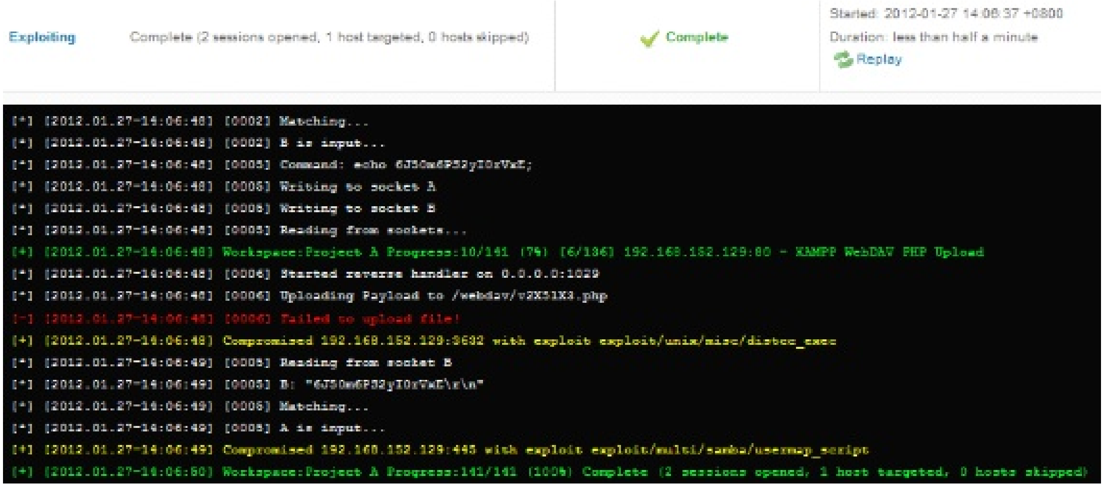
7.6 在 `Advanced Settings` （高级设置）部分下，您可以设置入侵行为，例如并发入侵 和超时。 启用 `Only obtain one session per target` （一个目标仅获取一个会 话）会将会话数限制为一个，即使主机具有多个漏洞允许创建多个会话也不例外。

至于 `Transport Evasion` （传输闪避）级别， `Low` （低）会在 TCP 数据包之间 插入延迟， `Medium` （中）将发送小型的 TCP 数据包， `High` （高）将应用这两 种闪避技术。 选择的级别越高，所需时间就越长，不过被检测到的几率也越低（例如 IDS）。

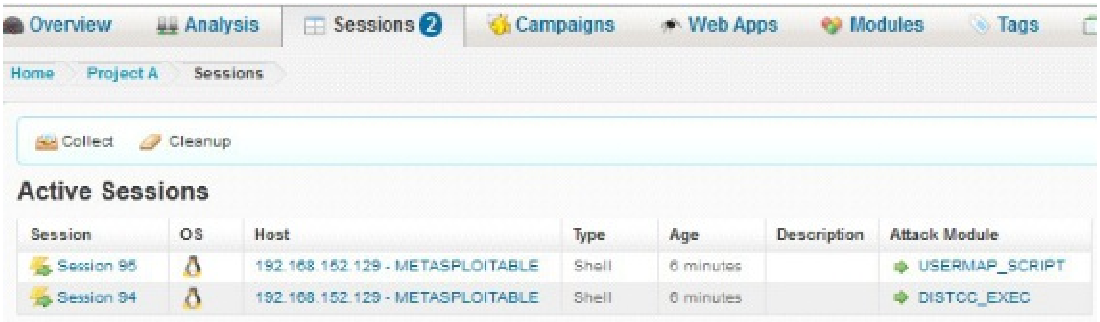
`Application Evasion` （应用程序闪避）这个闪避选项用于基于 DCERPC、SMB 和 HTTP 的入侵。 闪避选项越高级，闪避级别就越高。 `Dry run` （预检）将在任务 和日志中显示入侵信息。 不会进行实际的入侵。



7.7 点击右下角的 Exploit 来启动入侵任务。



如果入侵成功，就会在 `Session` （会话）选项卡上显示连接的会话和会话编号。



8. 控制会话

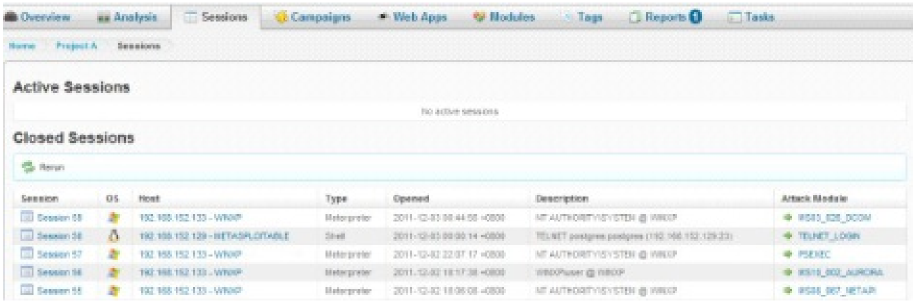
当您在目标系统上发现了有效的主机并获取了该系统上会话的访问权限，您就可以控制这 些打开的会话。 有两类会话：

Meterpreter 会话 – 这些会话的功能更强大。 不仅允许您利用 VNC 获取设备的访问权 限，还帮助您利用内置的文件浏览器上传/下载敏感信息。

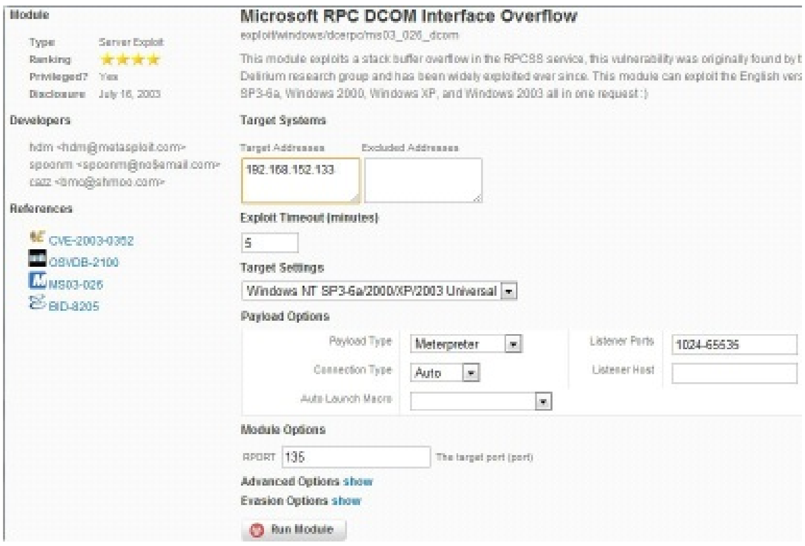
Command shell 会话 – 这些会话允许您对主机运行收集脚本，并通过外壳（shell）来 运行任意命令。

8.1 可以通过 `Exploit` （7.8 入侵章节）或 `Bruteforce` （6.10 强力攻击章节）来 构建会话。

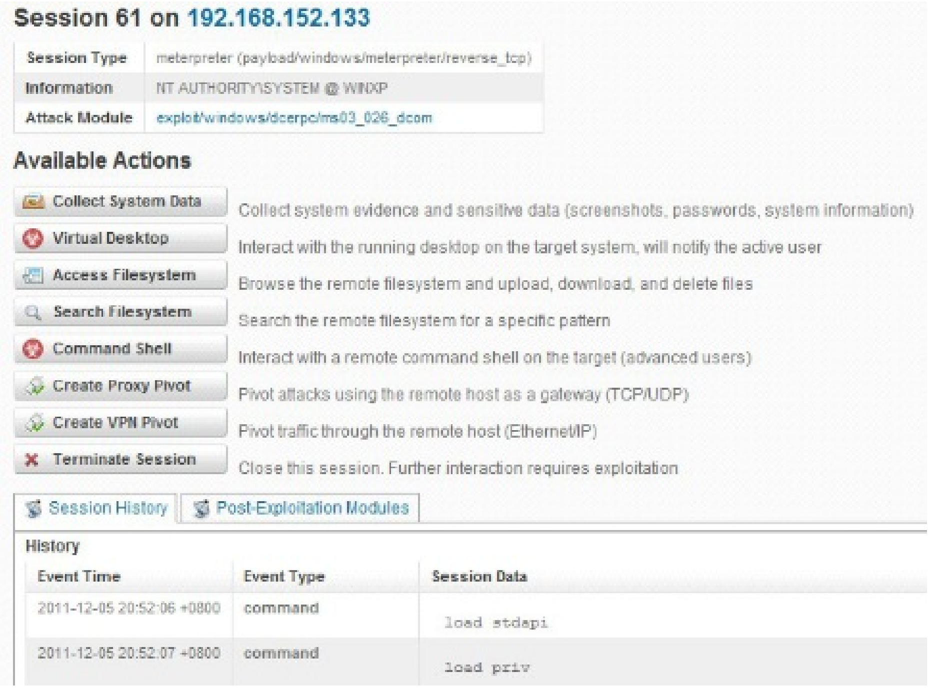
8.2 要重新打开会话，请前往 `Sessions` （会话）选项卡。 如果存在任何 `Active Sessions` （活动会话），则关闭所有这些会话。 点击其中一个已关闭会话的 `Attack Module` （攻击模块）。



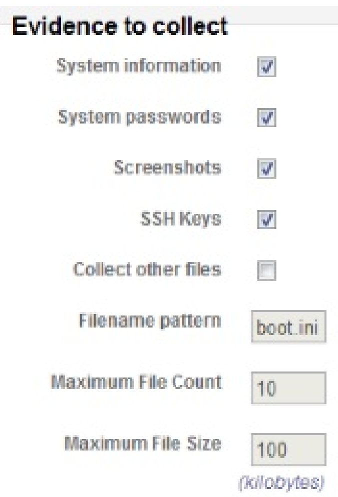
8.3 将显示模块详细信息、地址和有效载荷选项。 点击 `Run Module` （运行模块）再次 进行入侵。



8.4 Meterpreter 会话示例。 前往一个处于活动状态的会话。 为 Windows 使用 Meterpreter 有效载荷。 您可以点击 `Terminate Session` （终止会话）来关闭此 会话（不过现在不要执行该操作）。



8.5 收集证据： 获得访问权限后可以从目标自动收集证据。 可以使用这些证据执行进一步分析和渗透测试。 点击 Collect System Data 开始收集证据。 您可以选择收集 `System Information` （系统信息，即操作系统信息）、 `Passwords` （密码）、 `Screenshots` （屏幕截图）和 `SSH Keys` （SSH 密钥） 。 您也可以下载匹配模 式的文件。



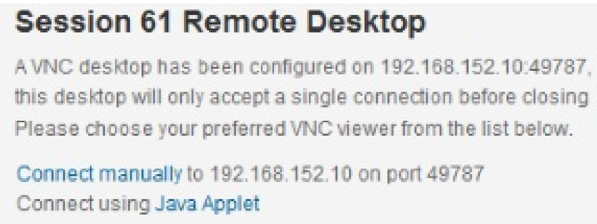
8.6 要检查从主机收集而来的证据，请前往 `Analysis > Hosts` （分析 > 主机）并从表 格中选择主机。 可以在 `Captured Evidence` （已捕获的证据）选项卡上找到这些 证据（例如：凭证和屏幕截图）。



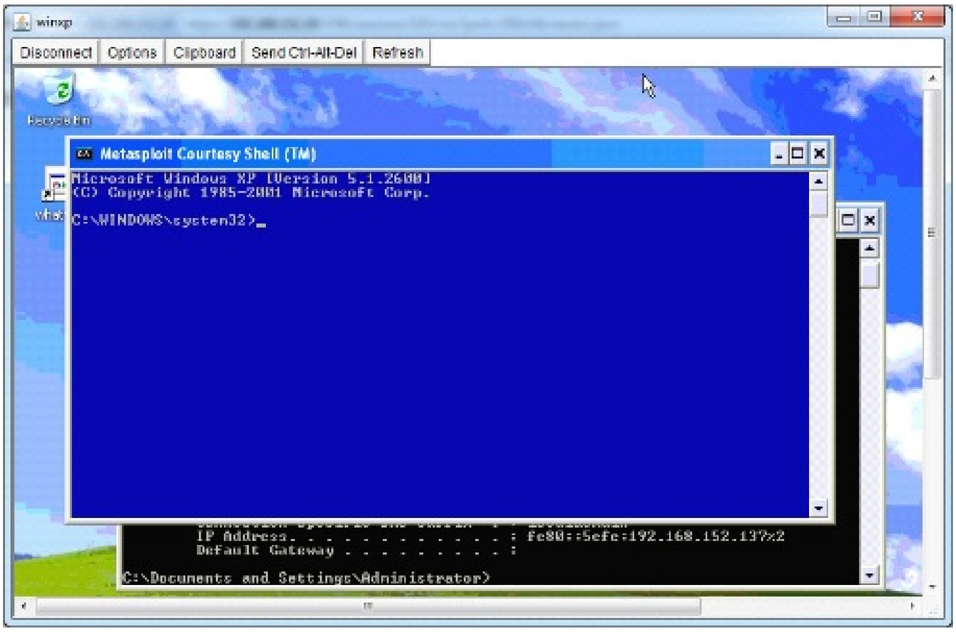
8.7 Meterpreter 会话将显示 Virtual Desktop ，允许您通过 VNC 会话连接到目标。 点击 `OK` （确定）来访问虚拟桌面。



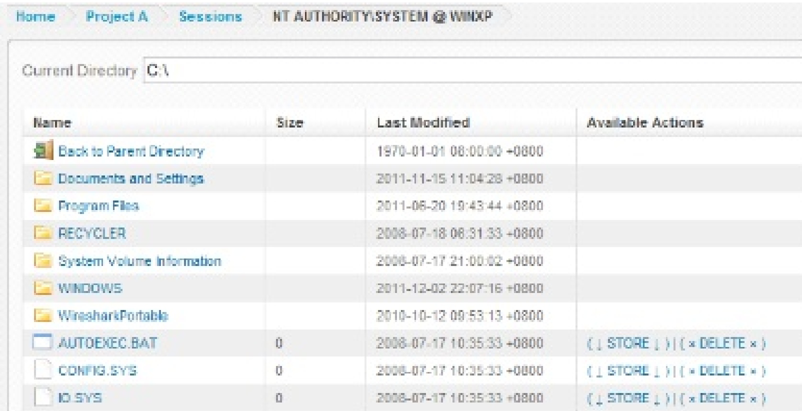
8.8 Metasploit Pro 拥有一个 Java 小程序形式的 VNC 客户端。 请为您的平台安装最新 的 Java。 此外还可以选择使用外部客户端（例如 VNC Viewer）。 点击蓝色的 `Java Applet` （Java 小程序）继续。



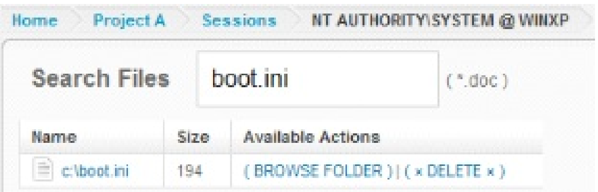
8.9 现在您就有了 VNC 会话。



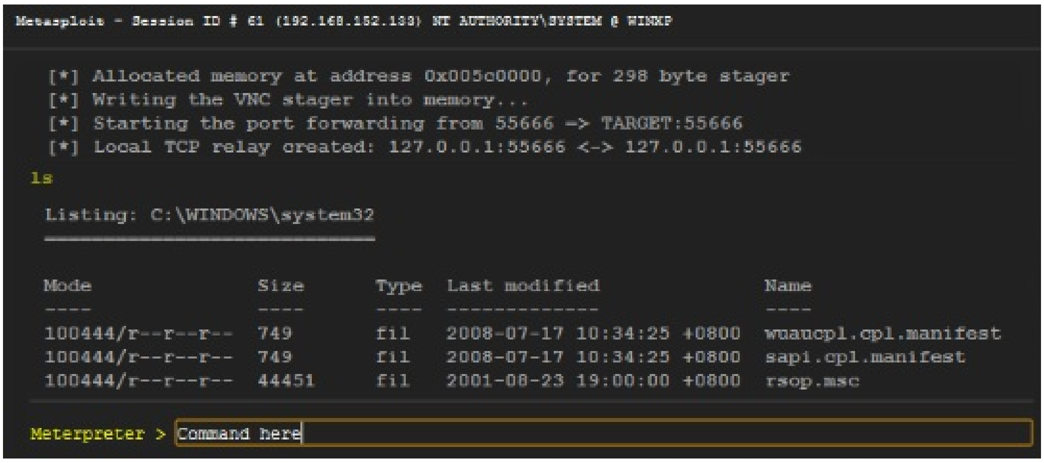
8.10 点击 Access Filesystem 来访问目标的文件系统。 Metasploit 将显示所有已映射的 驱动器。您可以浏览目录，下载、上传并删除作为证据的文件。



8.11 点击 Search Filesystem， 为特定的模式搜索远程文件系统。 这是寻找敏感文件的 有用工具。

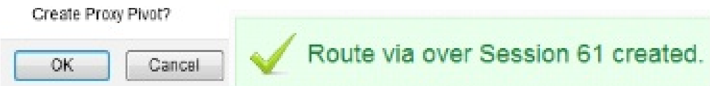


8.12 点击 Command Shell 与目标上的 Command Shell 进行交互。 使用 `help` （帮 助）来显示可用命令。它可以显示进程、浏览文件系统、使用 Webcam 等。



8.13 下方是 `getuid` 和 `getsystem` 命令的示例。



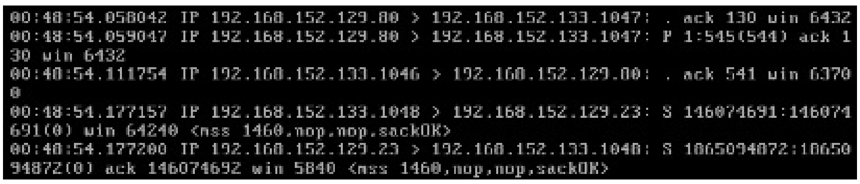


8.14 点击 Create Proxy Pivot 按钮来进行 Pivot Attack，将已入侵的主机（例如主机 A）作为网关（TCP/UDP）来入侵另一个主机（例如主机 B）。如果该攻击引起警报， 将看到远程主机（主机 A）， 而不是 Metasploit 主机。 点击 `OK` （确定）来继续 创建 Proxy Pivot。 如果创建成功，您将看见 `Route via over Session 61 created` （通过创建的会话 61 来进行路由）这条消息。

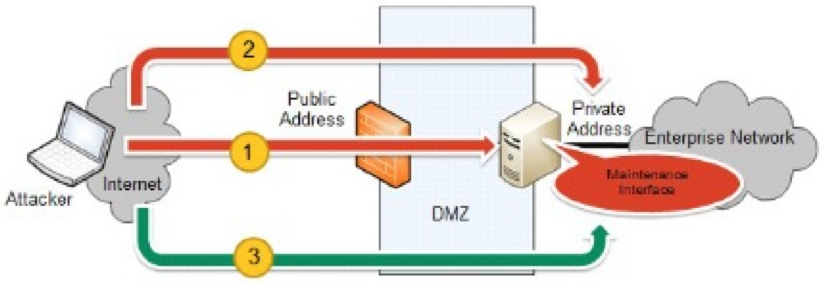
例如：Metasploit Pro（192.168.152.10）通过 WinXP 的 Proxy Pivot

（192.168.152.133）入侵目标 Metasploitable（192.168.152.129）。 从 Metasploitable 捕获的数据包来看，这些数据包只与 WinXP（而不是 Metasploit）

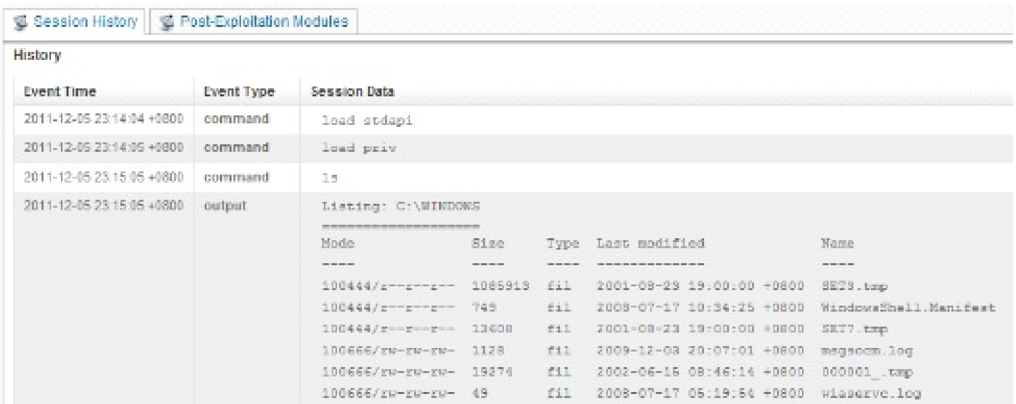
进行交换。



8.15 Create VPN Pivot 用来通过远程主机（Ethernet/IP）对通信量进行 Pivot Attack。通常，该功能用来入侵公共系统并交付 Meterpreter。 VPN Pivot 将利用与 远端受损主机建立的连接在攻击机器上创建接口。 要测试此功能，您需要准备一个具 有两个接口的 Windows 主机，一个接口连接到 Metasploit， 另一个接口连接到另一 个目标主机。



8.16 `Session History` （会话历史记录）选项卡显示已在运行哪些命令（例如 VNC）和脚本（例如 VPN.rb）以及输出信息（例如：浏览文件系统）。



8.17 `Post-Exploitation Modules` （入侵后模块）选项卡列出可以在此会话上运行 的所有可用模块。 可以从以下链接找到脚本库。

http://www.metasploit.com/redmine/projects/framework/repository/show/scripts/meter preter

8.18 要运行一个模块，请找到 `Windows Gather Product Key` （Windows 收集产品密

钥）并点击 Run Module。 若成功，将在 `Stored Data & Files` （已存储数据和 文件）选项卡上显示密钥。

Home Project A Modules Windows Gather Product Key

---

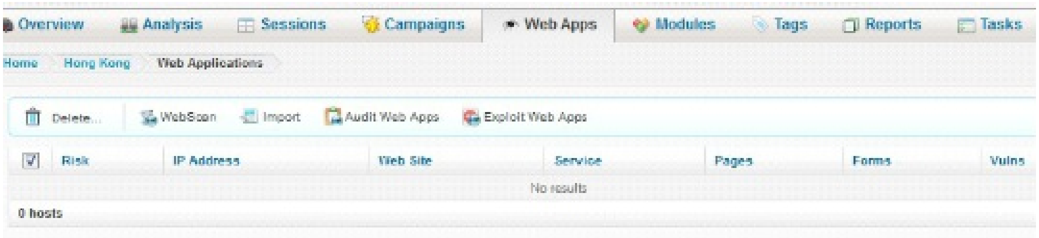
9. Web 应用程序测试

Metasploit Pro 在 Web Apps （Web 应用程序）选项卡下提供 Web 扫描、Web 审 计和 Web 入侵功能。 这些功能帮助您在处于活动状态的 Web 内容和表单中搜索漏洞 并进行入侵。

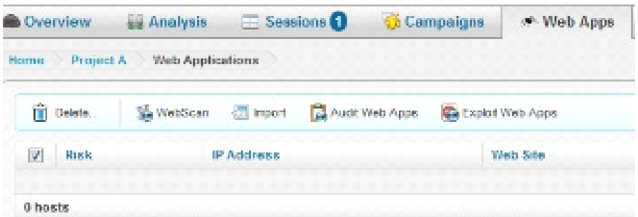
- Web 应用程序扫描： 对网页启用爬虫、搜索表单和活动内容
- Web 应用程序审计： 搜索这些表单中的漏洞
- Web 应用程序入侵： 入侵找到的漏洞

9.1 点击 

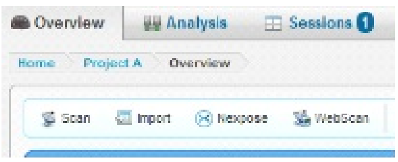
选项卡前往 Web Apps （Web 应用程序） 页面。

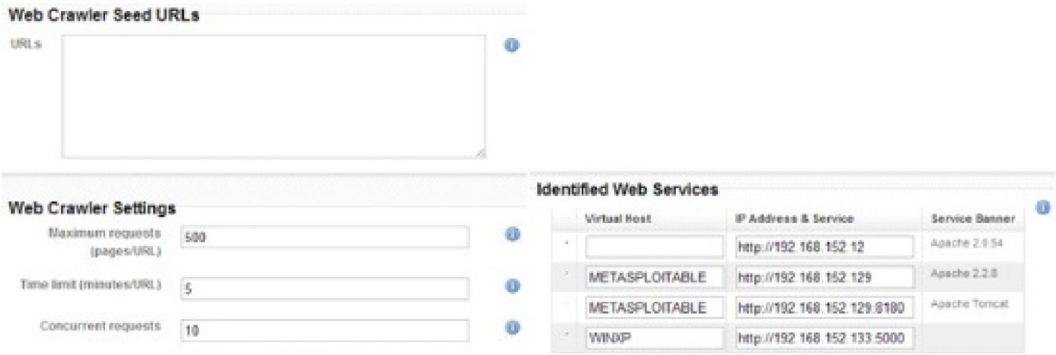


9.2 要运行 web 扫描，请前往 Web Apps > WebScan 或 Project > WebScan （项目 > WebScan）。

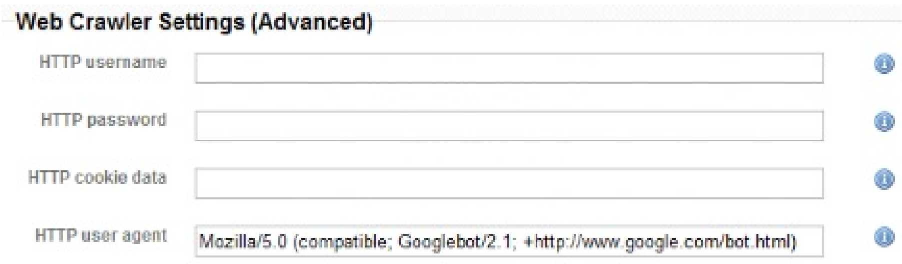


9.3 输入条件，包括 Seed URLs （种子 URL）、 Max # pages requested （请求的 最大页数）、 Max amount of time （最长时间）、 # of concurrent requests 、 allowed per website （每个网站允许的并发请求数量）。 从过去的扫描中选择已 识别的 web 服务。

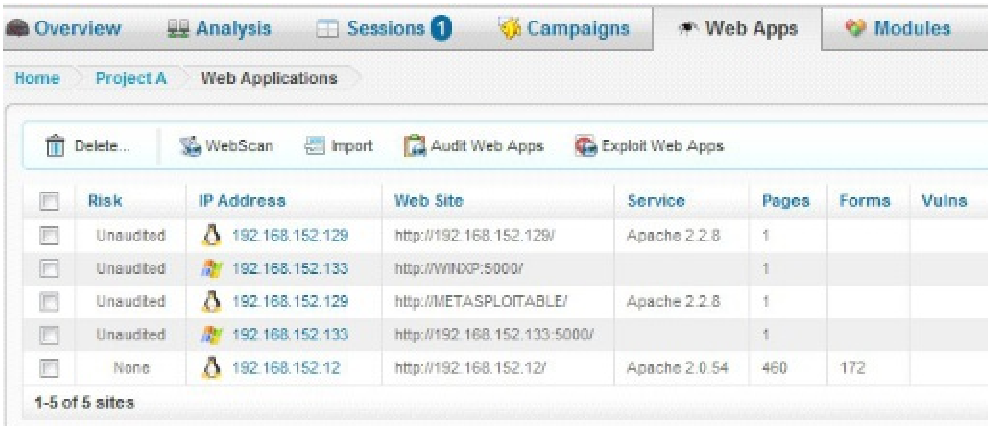




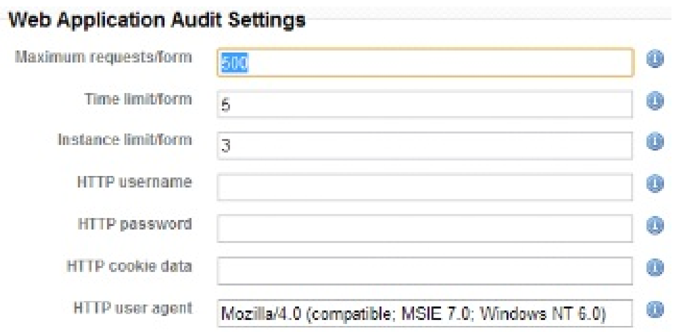
9.4 要为 HTTP 基本验证和 cookie 输入凭证，请点击 Show Advanced Options 按钮。



9.5 点击 Launch Scan 按钮来启动 web 扫描。 扫描后，将在 `Web Apps` （Web 应用程 序）选项卡上显示找到的 Web 应用程序。 这些信息包括 IP 地址、网站 URL、服务 名称、 页数和表单数量。



9.6 要运行 Web 审计来搜索已扫描表单中的漏洞，请点击 Audit Web Apps 按钮。 输入您 的条件，包括 `Max # requests sent to target application form` （发送至目标 应用程序表单的最大请求数量）、 `Max amount of time per form` （每个表单的最 长时间）、 `Max # of unique form instances` （唯一表单实例的最大数量）、 `Credential information` （凭证信息）和 `User agent` （用户代理程序）。

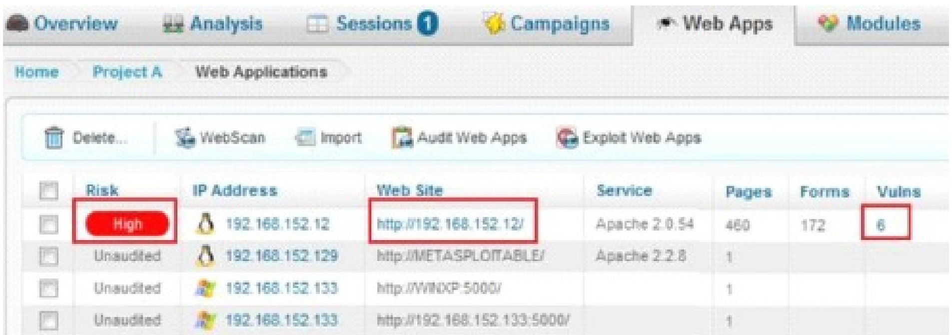


9.7 您也可以选择 `Target Web App` （目标 Web 应用程序）。

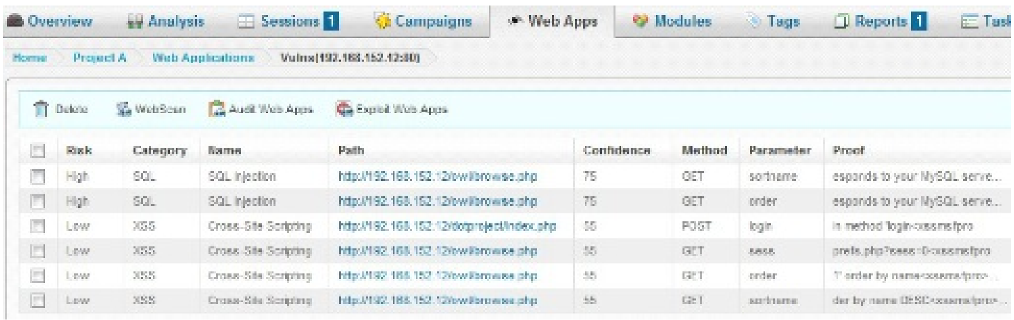


9.8 点击 Launch Audit 按钮来启动 web 审计。 将在 `Web Apps` （Web 应用程序）选项 卡上更新 Web 审计结果，例如漏洞数量。 点击 `Risk` （风险）图标， `Vulns`

（漏洞）数量或 `Web Site` （网站）URL 来检查 web 应用程序的漏洞列表。



9.9 将通过以下信息显示具有漏洞的 web 应用程序，包括漏洞类型（例如 SQL 注入）、 路径、机密性级别、所用方式、参数和证据。



9.10 要通过漏洞入侵 web 应用程序，请点击漏洞详细信息的 `Path` （路径）。 例 如：选择一个属于 XSS 类 别的漏洞。 利用 `VULNERABLE` 这个单词定位登录字段， 并通过在 `VULNERABLE` 后添加一些信息来编辑该字段。



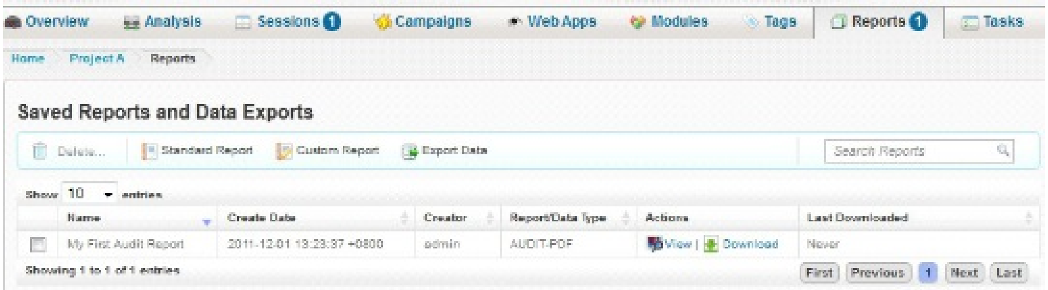
9.11 点击 Replay XSS Attack 。该浏览器将显示已被注入的网页。



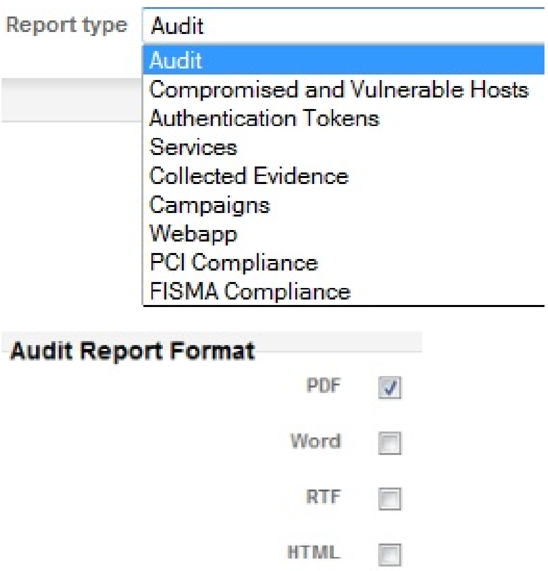
10. 报告

报告页面提供一列实时 HTML 报告和生成的报告。 可以导出并保存这些生成的统计报 告。

10.1 点击 `Reports` （报告）选项卡来生成报告并进行查看。

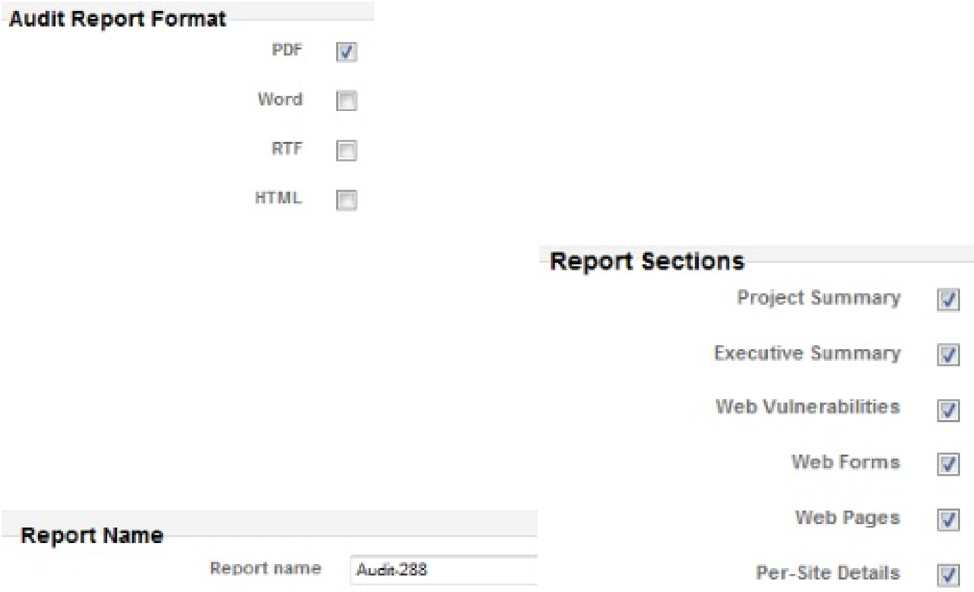


10.2 点击 `Standard Report` （标准报告）来生成报告。 提供 9 种内置的报告类型， 请选择一种类型。 要了解各类报告的详细信息，请将鼠标悬停在 图标上。

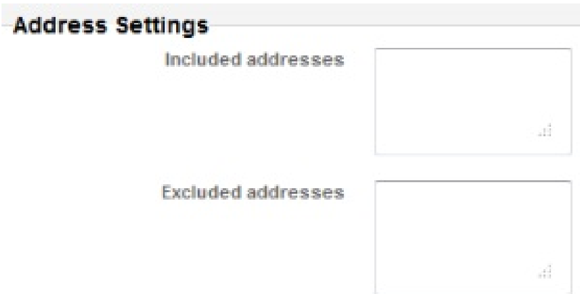


10.3 取决于报告类型，将显示相应的选项。 输入报告名称。

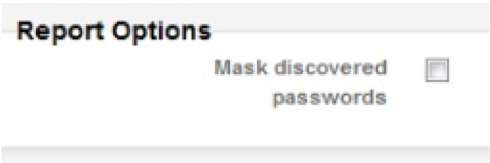
- 格式（例如 XML 格式的 `PCI 合规报告` ）
- 组成部分（例如 `服务报告` 中的 `网络服务表格` 部分）
- 选项（例如在 `验证令牌报告` 中 `隐藏已发现的密码` ）



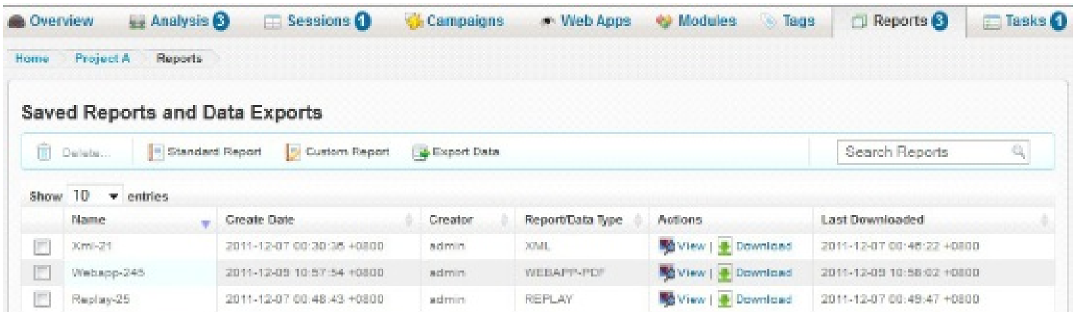
10.4 自定义要在报告中包含或排除的 IP 地址。 您也可以删除一些组成部分。



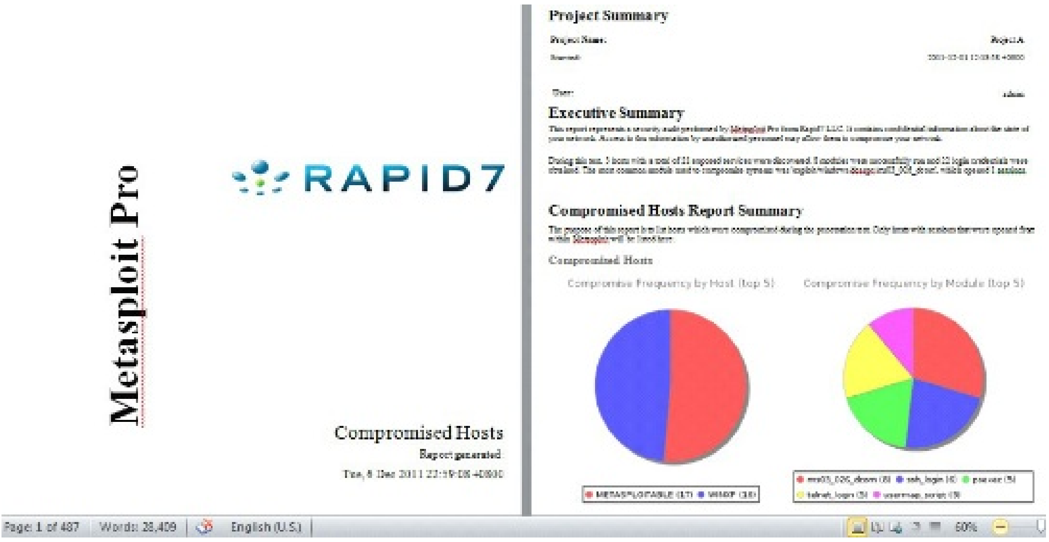
10.5 取决于报告类型，将提供不同的 `Report Options` （报告选项）并显示不同的 `Generate Report` （生成报告）按钮。 点击 Generate Webapp Report 来生成报告。



10.6 一旦完成报告生成任务，请前往 `Report` （报告）选项卡，其中将显示所有已生 成的报告。 您可以查看或下载报告。



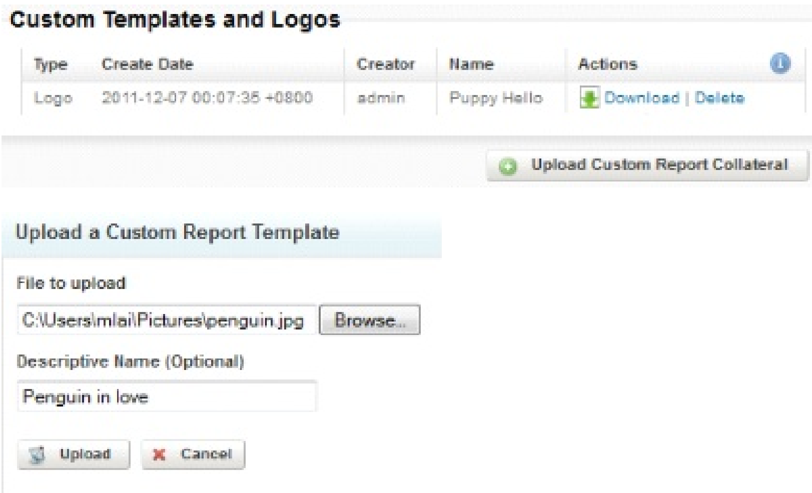
10.7 良好的习惯是限制报告的输出（例如：排除某些 IP），因为报告可能有 100 多页或 1000 多页。



10.8 要生成自定义报告，请点击 `Reports` （报告）选项卡上的 Custom Report 。 可以 使用报告模板和徽标对报告进行定制。 可以从 `Reports` （报告） 页面底部下载模 板。



10.9 点击 Upload Custom Report Collateral 来上传徽标或模板。 选择要上传的文件并输入描 述。 点击 Upload 开始上传。



10.10 在 `Custom Report Settings` （自定义报告设置）部分下，选择 `Custom report logo` （自定义报告徽标）。 也可以在 `Standard Reports` （标准报告） 中使用自定义徽标。



10.11 Metasploit 允许导出数据。 点击 Export Data 来生成在渗透测试期间找到的所有 数据。 数据的导出格式包括 PDF、XML、RTF、ZIP、PWDump 或 Replay 脚本，可以进 行下载。

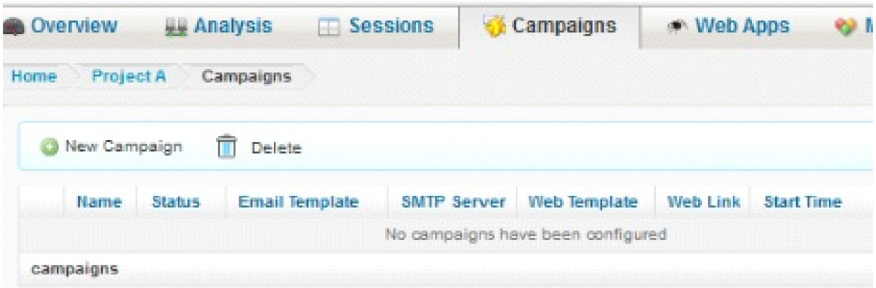
11. 社会工程

在 Metasploit Pro 中使用 `Campaigns` （宣传活动）来启动 `Social Engineering`

（社会工程）。 `Campaign` （宣传活动）包括 Web、电子邮件和 USB 模式。 您可以 自定义网页和电子邮件内容来模拟面向客户端的常规钓鱼攻击。 一旦目标客户端连接到

Metasploit Pro 服务器，就可以自动运行客户端入侵模块。

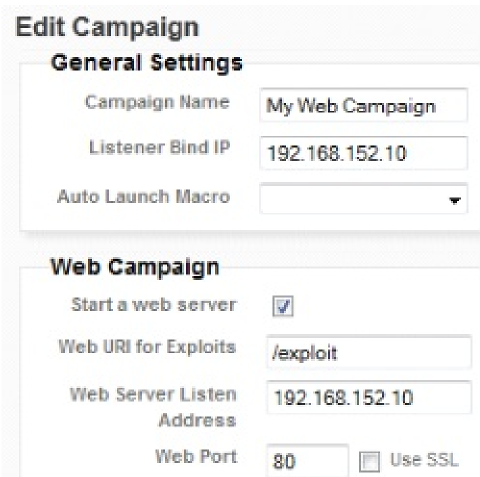
11.1 点击 Campaigns 选项卡进入 `Campaigns` （宣传活动） 页面。



11.2 点击 New Campaign 来新建一个宣传活动。 输入 `Campaign Name` （宣传活动名 称） 和 `Listener Bind IP` （监听程序绑定 IP） 。 要启动一个 Web Campaign

（Web 宣传活动） ， 勾选 `Start a web server` （启动 web 服务器） ， 输入 URI

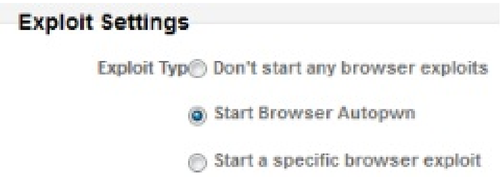
（可选） 、Web 服务器 IP 和端口。



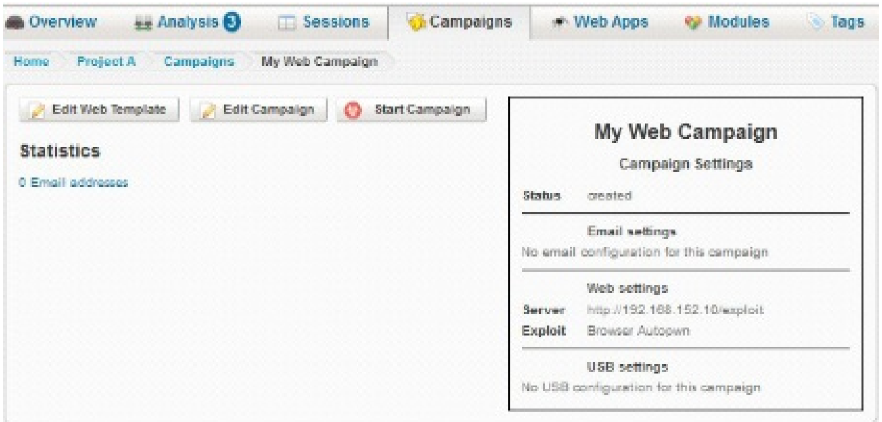
11.3 一旦保存完毕，您将看到 `Create a web template for this campaign` （为此 宣传活动创建一个 web 模板） 页面，因为已在上一步中选择 `Start a web server` （启动 web 服务器） 。 您可以编辑 HTML 模板。 要克隆一个 URL，请输入 URL 并点击 Clone URL ，将显示已克隆 URL 的 HTML 代码。



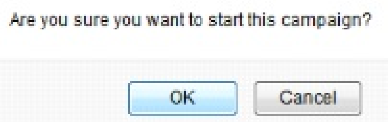
11.4 在 `Exploit Settings` （入侵设置）部分下， `Start Browser Autopwn` （启 动浏览器 Autopwn）会自动发送相关客户端浏览器和操作系统指纹的入侵。 您可以选择 `Start a specific browser exploit` （启动特定的浏览器入侵）来测试特定的 客户端模块（例如 Aurora）。 或者您可以选择 `Don't start any exploit` （不 启动任何入侵）， 不执行任何操作。



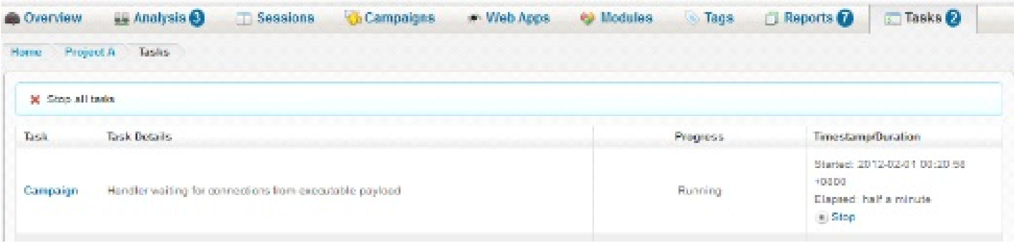
11.5 Save 选择 `Start Browser Autopwn` （启动浏览器 Autopwn）。 并点击 Start Campaign 。 Rerun Campaign 可以启动、停止和再次运行宣传活动。点击 Stop Campaign 。



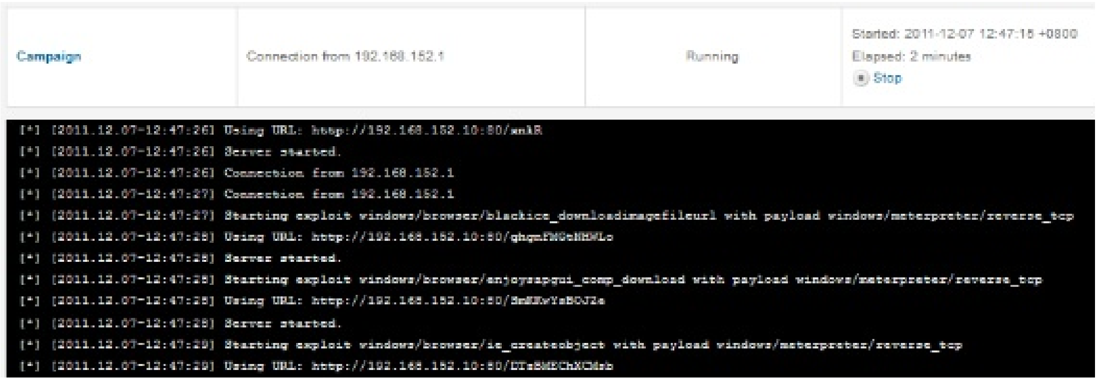
11.6 点击 Start Campaign 和 `OK` （确定）来启动宣传活动。



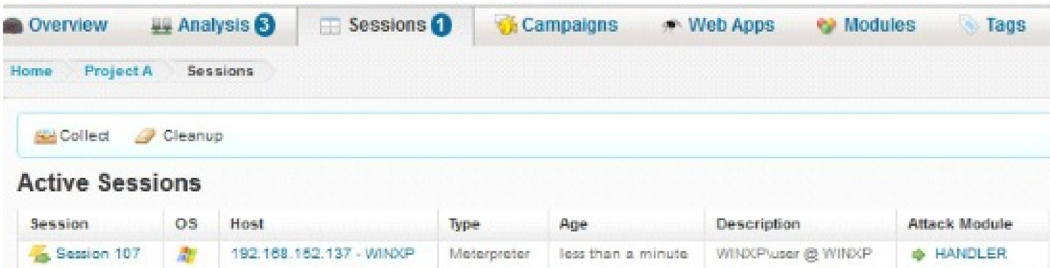
11.7 该宣传活动在 `Tasks` （任务）选项卡下运行。



11.8 尝试从目标客户端的浏览器访问 Web Campaign URL（Web 宣传活动 URL）。 任务日志将显示入侵信息。



11.9 如果入侵成功，将构建新的会话。



12. 高级技术

本章节将说明 `Post-Exploitation Macros` （入侵后宏）和 `Persistent Agent` （持 续代理程序）。 `Post-Exploitation Macros` （入侵后宏）帮助您在构建完会话后自 动执行操作。 例如：通过 XP 工作站构建完一个会话后，无需管理员的介入即可自动执 行密码收集和屏幕捕获操作。

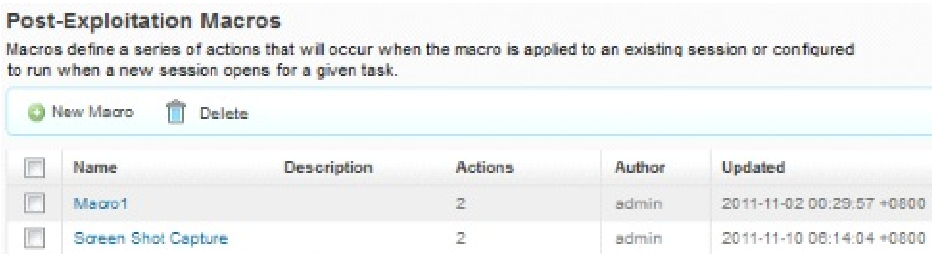
`Persistent Agent` （持续代理程序）帮助您在重启和登录主机后，让主机自动构建针 对 Metasploit 的会话。无需再次入侵/强力攻击主机。 换言之，在 Metasploit 的控制 下，部署了代理程序的主机就像是 `僵尸` 。

12.1 将鼠标移至顶部菜单栏上的 Administration ▼ 选项卡并点击 Global Settings 。

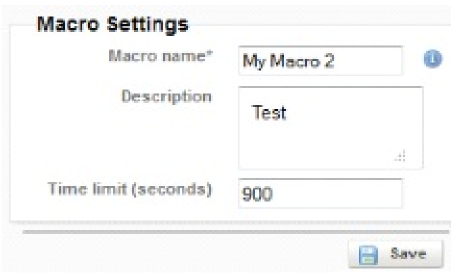


12.2 在 `Global Settings` （全局设置）页面上的 `Post-Exploitation Macros`

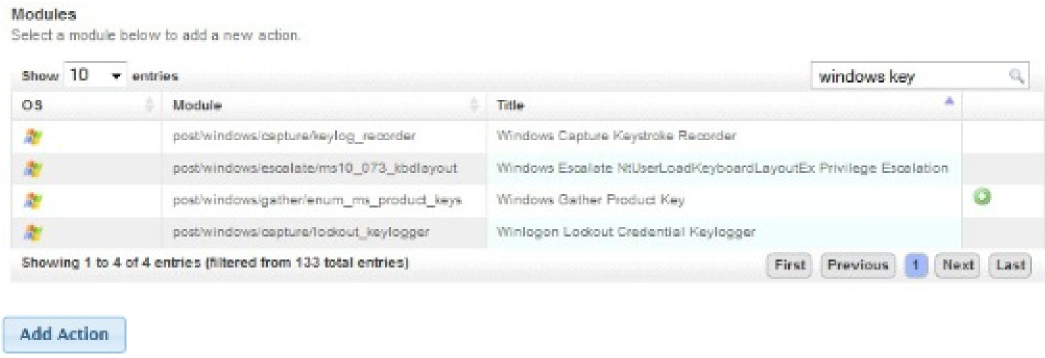
（入侵后宏）部分中，点击 New Macro 来添加一个新的宏。



12.3 输入名称和描述并点击 Save ，然后就会显示供选择的模块。



12.4 您可以按关键字（例如 windows key）来搜索模块。 将鼠标移至选定模块（例 如：Windows Gather Product Key）的最后一栏，将显示，点击该图标为此新宏添 加一个操作。



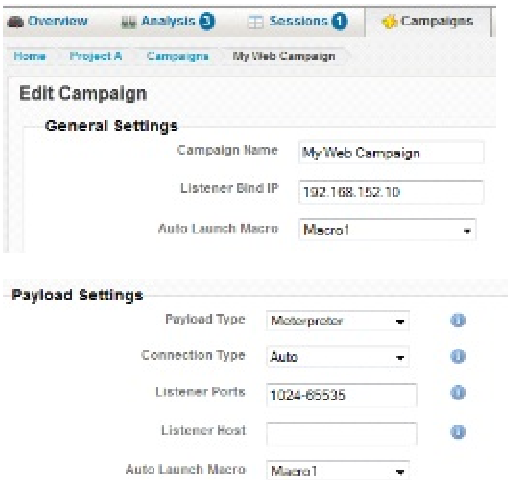


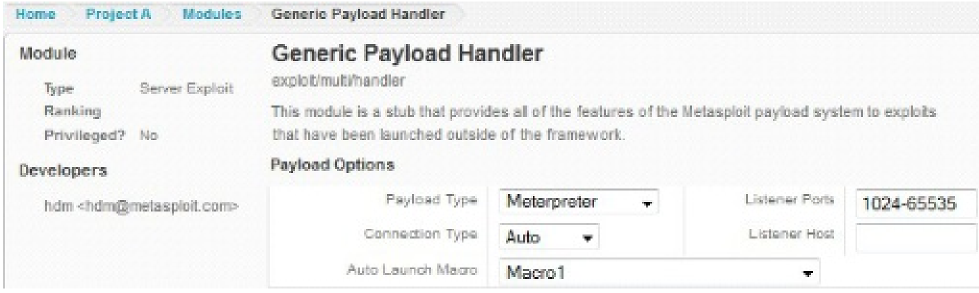
12.5 点击 Add Action 进行确认，以便将选定的操作添加到此宏。

12.6 将在上方表格中显示已添加的操作。 点击 Update Macro 来保存设置。



12.7 在构建完会话时可以自动启动宏。 您可以在 `Exploit` （入侵，7.4 章节）、 `Bruteforce` （强力攻击，6.6 章节） （ Bruteforce Exploit ）、 `Campaigns > General Settings` （宣传活动 > 常规设置， 11.2 章节）中的 `Advanced Section > Payload Settings` （高级部分 > 有效载荷设置）下选择 `Macro` （宏），也可 以在各个模块的 `Payload Options` （有效载荷选项）中选择这些宏。





12.8 在 `Persistent Listeners` （持续监听器）部分下，您可以添加监听器来让客户端自动回连。 点击  。

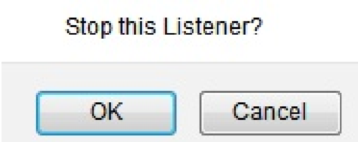


12.9 选择一个项目来与此监听器相关联。 选择 `Listener Payload` （监听器有效载荷）、 `Address` （地址）和 `Port` （端口）。 一旦远程主机回连，即可自动加 载宏。

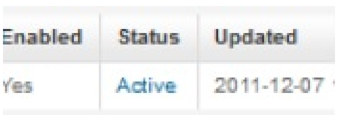


12.10 点击  ，即可在选定的项目上找到 `Listening` （监听）任务。



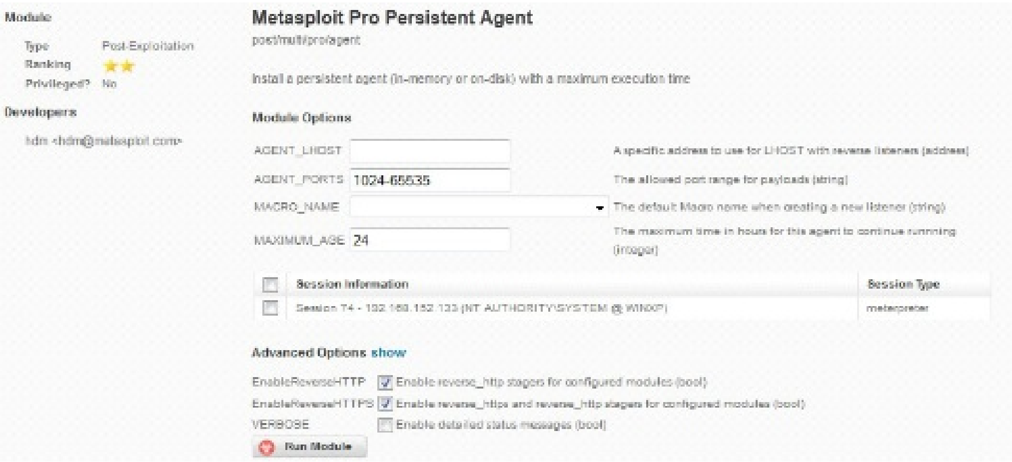


12.11 可以通过点击 `Inactive/Active` （闲置/活动）状态来启动/停止监听器。

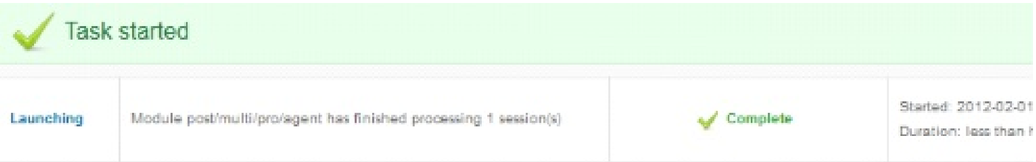


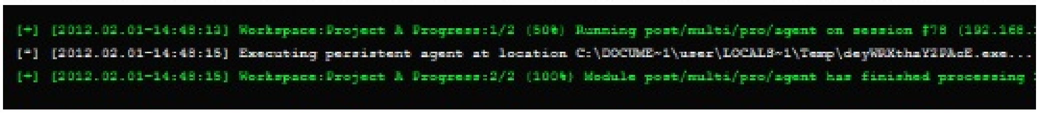
12.12 现在 母舰 已准备就绪，下一步是部署持续代理程序，以便让客户端回连。 在 针对 WinXP 的活动会话中，运行入侵后模块 `Metasploit Pro Persistent Agent` （Metasploit Pro 持续代理程序）。



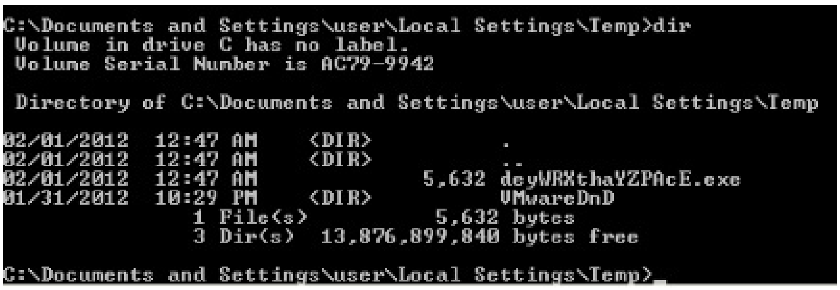


12.13 选择会话并点击 Run Module 。 您将在任务日志上看到目标对象中的代理程序位 置（例如：c:.....\ajlkfljdsaf.exe）。

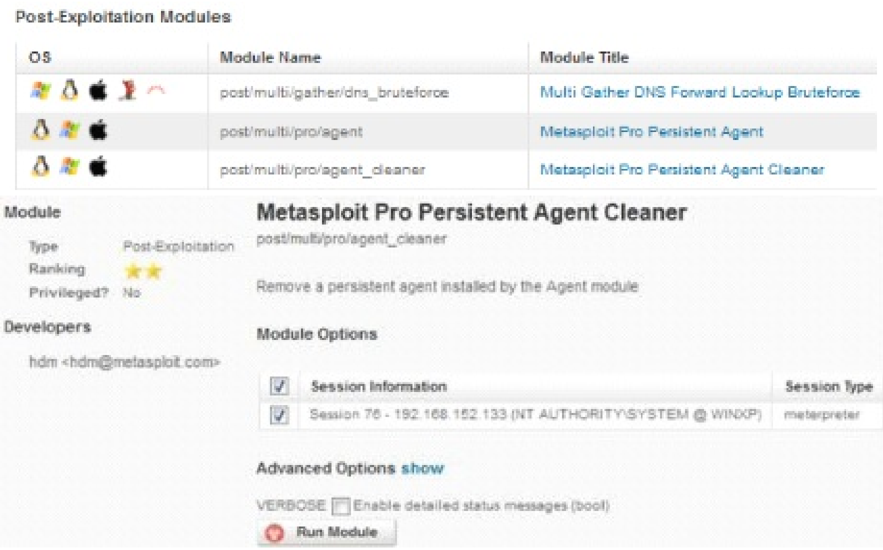




12.14 前往目标文件系统，并检查是否存在这个代理程序。



12.15 重启 WinXP 目标并再次登录。 您将看到会话的自动构建。



12.16 要删除代理程序，您可以运行入侵后模块 `Metasplit Pro Persistent Agent Cleaner` （Metasplit Pro 持续代理程序清除器）。